Getting in on the Act:

The Review of the Private Sector Provisions of the Privacy Act 1988

March 2005
The Hon Philip Ruddock MP
Attorney-General
Parliament House
CANBERRA ACT 2600

Dear Attorney-General

I refer to your request of 13 August 2004 asking me to undertake a review of the private sector provisions of the Privacy Act 1988.

I have pleasure in presenting to you the report: *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988.*

Yours sincerely

Karen Curtis
Privacy Commissioner

31 March 2005
# Table of Contents

Foreword ........................................................................................................................................ viii

Overview and Executive Summary................................................................................................. 1
  Approach to the review............................................................................................................... 1
  Terms of reference.................................................................................................................... 1
  Participants in the review ......................................................................................................... 1
  Timing of the review.................................................................................................................. 1
  Provisions work well on balance .............................................................................................. 2
  A single national scheme .......................................................................................................... 4
  Main recommendations ............................................................................................................ 6

Recommendations:......................................................................................................................... 8
  Recommendation: Wider review of Privacy Act ......................................................................... 8
  Recommendations: National consistency .................................................................................... 8
  Recommendations: Telecommunications consistency ................................................................. 9
  Recommendations: Health consistency ....................................................................................... 9
  Recommendations: Residential tenancy databases ................................................................... 9
  Recommendation: EU 'adequacy' and APEC ............................................................................. 10
  Recommendation: NPP 9........................................................................................................... 10
  Recommendations: Control over personal information .................................................................. 10
  Recommendations: Direct marketing ........................................................................................ 10
  Recommendations: Consumer education ................................................................................... 11
  Recommendations: Access generally ....................................................................................... 11
  Recommendations: Transfer of health records .......................................................................... 12
  Recommendations: Health service ceases to operate ................................................................. 12
  Recommendations: Complaints handling and compliance ......................................................... 13
  Recommendation: Approved privacy codes .............................................................................. 14
  Recommendations: Business awareness .................................................................................... 14
  Recommendations: Small business exemption ........................................................................... 15
  Recommendations: Private sector contracting .......................................................................... 15
  Recommendation: Due diligence ............................................................................................... 15
  Recommendations: Media exemption ......................................................................................... 15
  Recommendations: Research ..................................................................................................... 16

Recommendations: Decision-making where capacity is impaired .............................................. 16
  Recommendation: Law enforcement ........................................................................................ 17
  Recommendation: Private investigations ................................................................................... 17
  Recommendations: Alternative dispute resolution schemes ................................................... 17
  Recommendations: Large scale emergencies ............................................................................ 18
  Recommendations: New technologies ........................................................................................ 18
  Recommendation: NPP 1.3(d).................................................................................................. 19
  Recommendation: Reasonable steps for NPP 1.3 and 1.5 ......................................................... 19
  Recommendation: NPP 1.5 – ‘Someone’ .................................................................................... 19
  Recommendations: Primary purpose and health information .................................................. 20
  Recommendation: NPP 3 – Data quality .................................................................................... 20
  Recommendation: NPP 7 - Identifiers ....................................................................................... 20
  Recommendations: NPP 10 – Public Interest Determinations ................................................... 20
  Recommendations: NPP 10.2(b)............................................................................................... 21
  Recommendations: Deceased persons ...................................................................................... 21

1 Background ................................................................................................................................ 22
  1.1 This Inquiry .......................................................................................................................... 22
  Background to the review .......................................................................................................... 22
  Terms of Reference..................................................................................................................... 22
Matters not included in the review ................................................................. 22
Other relevant privacy related reviews and processes ......................... 23
Research .................................................................................................. 23
Framework for assessing issues ............................................................... 23
Conduct of the review- overview of consultation ...................................... 24
Issues Paper ............................................................................................ 25
Consultation Meetings ............................................................................. 25
Written Submissions ............................................................................... 26
Structure of report .................................................................................. 26

1.2 Private Sector Provisions of the Privacy Act ........................................ 27
History of Commonwealth Privacy Legislation ....................................... 27
What do the Private Sector Provisions cover? ......................................... 29

2 National Consistency .............................................................................. 32
2.1 National consistency overall ............................................................... 32
National consistency was goal of legislation ........................................... 32
Issues ..................................................................................................... 32
Other law impacting on privacy ............................................................... 33
Submissions favour national consistency ............................................... 35
What submissions say - issues ............................................................... 37
What submissions say – addressing the issues ........................................ 42
Options for reform ................................................................................ 45

2.2 Recommendations: National consistency .......................................... 48
2.3 Consistency in telecommunications ................................................... 49
Law and policy ...................................................................................... 49
Complaints and enquiries ....................................................................... 51
What the submissions say - issues ......................................................... 53
What submissions say – addressing the issues ........................................ 57
Options for reform ................................................................................ 58

2.4 Recommendations: Telecommunications consistency ...................... 63
2.5 Consistency in protection of health information ............................... 64
Law and policy ...................................................................................... 64
What the submissions say - issues ......................................................... 65
Options for reform ................................................................................ 68

2.6 Recommendations: Health Consistency .......................................... 71
2.7 Residential tenancy databases .......................................................... 72
What are residential tenancy databases? ............................................... 72
Application of the Privacy Act ............................................................... 72
Issues ..................................................................................................... 72
Options for reform ................................................................................ 72

2.8 Recommendations: Residential tenancy databases .......................... 73

3 International issues and obligations ...................................................... 74
3.1 EU Adequacy and APEC ................................................................. 74
Law and Policy ...................................................................................... 74
Issues ..................................................................................................... 75
What submissions say - issues ............................................................... 75

3.2 Recommendation: EU ‘adequacy' and APEC .................................... 76
3.3 NPP 9 ............................................................................................... 76
Law and policy ...................................................................................... 76
Issues ..................................................................................................... 77
What submissions say – issues ............................................................... 77
What submissions say – addressing the issues ........................................ 78
Options for reform ................................................................................ 79

3.4 Recommendation: NPP 9 ............................................................... 80
4 Protecting individual’s right to privacy .............................................................. 81
  4.1 Control over personal information ................................................................. 81
     Law and policy .......................................................................................... 81
     Issues ....................................................................................................... 81
     Community attitudes survey .................................................................... 82
     What submissions say - issues .................................................................. 83
     What submissions say – addressing the issues ......................................... 89
     Options for reform .................................................................................. 91
  4.2 Recommendations: Control over personal information ............................ 93
  4.3 Direct marketing .......................................................................................... 94
     What is direct marketing? ......................................................................... 94
     Law and policy ........................................................................................ 94
     Rationale ................................................................................................ 95
     Community attitudes survey .................................................................... 96
     Issues ....................................................................................................... 96
     What submissions say – the issues ............................................................ 96
     What submissions say – addressing the issues ........................................ 100
     Options for reform ................................................................................. 102
  4.4 Recommendations: Direct marketing .......................................................... 103
  4.5 Awareness of, confidence in and capacity to exercise rights ...................... 104
     Law and policy ........................................................................................ 104
     Issues ....................................................................................................... 104
     Role of the Office .................................................................................... 105
     Role of organisations .............................................................................. 105
     Community awareness survey ................................................................ 105
     Demographic information about complainants ..................................... 106
     What submissions say - issues ................................................................. 107
     What submissions say – addressing the issues ....................................... 108
     Options for reform ................................................................................ 110
  4.6 Recommendations: Consumer education .................................................... 111
  4.7 Access generally ......................................................................................... 112
     Law and policy ........................................................................................ 112
     Issues ....................................................................................................... 112
     What submissions say - issues ................................................................. 113
     What submissions say – addressing the issues ....................................... 115
     Options for reform ................................................................................ 117
  4.8 Recommendations: Access generally .......................................................... 118
  4.9 Transfer of health records to another health service provider .................... 119
     Law and policy ........................................................................................ 119
     What submissions say ............................................................................... 119
     Options for reform ................................................................................ 119
  4.10 Recommendations: Transfer of health records .......................................... 121
  4.11 Access to health records when health service ceases to operate .............. 122
     Law and policy ........................................................................................ 122
     Health services ceasing to operate .......................................................... 122
     What submissions say ............................................................................... 123
     Options for reform ................................................................................ 123
  4.12 Recommendations: Health service ceases to operate .............................. 124

5 Enforcing individual rights and ensuring compliance .................................... 125
  5.1 Introduction ............................................................................................... 125
  5.2 Law and policy ......................................................................................... 125
     Approach to compliance .......................................................................... 125
     Complaints process .............................................................................. 126
6 Balancing individual privacy interests with business efficiency .......... 164

6.1 Introduction ................................................................. 164
Law and policy................................................................. 164
Issues ............................................................................. 164
Striking the balance......................................................... 164
Principles or rules............................................................. 165
Principles may need some illumination ............................ 165

6.2 Approved Privacy Codes ................................................... 166
Law and policy................................................................. 166
Issues ............................................................................. 166
What submissions say - issues ........................................... 167
What submissions say – addressing the issues .................... 169
Options for reform........................................................... 170

6.3 Recommendation: Approved Privacy Codes ....................... 171

6.4 Compliance costs .......................................................... 171
Law and policy................................................................. 171
Issues paper ................................................................. 171
What submissions say ...................................................... 172

6.5 Business awareness ....................................................... 175
Issues ............................................................................. 175
What submissions say ...................................................... 175
Options for reform........................................................... 177

6.6 Recommendations: Business awareness ......................... 178

6.7 Small business exemption ............................................. 179
Law and policy................................................................. 179
Issues ............................................................................. 179
7 Balancing individual rights and other social interests

7.1 Media exemption
7.2 Medical research
7.3 Decision-making where capacity is impaired
7.4 Recommendations: Research
7.5 Recommendations: Medical research
7.6 Recommendations: Decision-making where capacity is impaired
7.7 Law enforcement
7.8 Recommendations: Law enforcement
7.9 Private investigation
7.10 Recommendations: Private investigations
7.11 Alternative Dispute Resolution
7.12 Recommendations: Alternative dispute resolution schemes
7.13 Responding to large scale emergencies
9.18 NPP 10 – Collection of Family History Information – PID 9 and 9A ........................................ 273
Law and Policy .................................................................................................................. 273
What the submissions say – issues................................................................................... 275
Options for Reform ......................................................................................................... 276
9.19 Recommendations: NPP 10 – Public Interest Determinations ................................. 277
9.20 NPP 10.2 – Collecting health information without consent ...................................... 277
Law and Policy .................................................................................................................. 277
Scope of the exception ...................................................................................................... 278
Options for Reform ......................................................................................................... 279
9.21 Recommendations: NPP 10.2(b) ............................................................................ 280

10 Other issues with the private sector provisions of the Privacy Act ......................... 281
10.1 Information of deceased persons ............................................................................ 281
Law and Policy .................................................................................................................. 281
What submissions say – issues........................................................................................ 282
Options for Reform ......................................................................................................... 283
10.2 Recommendations: Deceased persons .................................................................. 284
10.3 Employee Records Exemption .............................................................................. 285
Law and Policy .................................................................................................................. 285
What submissions say...................................................................................................... 285
10.4 Political Exemption .................................................................................................. 285
Law and Policy .................................................................................................................. 285
What submissions say...................................................................................................... 286

Appendix 1287
Terms of Reference ............................................................................................................ 287
Appendix 2288
Review Reference Group .................................................................................................. 288
Appendix 3290
Submissions Received ....................................................................................................... 290
Appendix 4293
National Privacy Principles .............................................................................................. 293
Appendix 5305
Information Privacy Principles .......................................................................................... 305
Appendix 6311
Community Attitudes towards Privacy 2004 ................................................................... 311
Appendix 7317
Information Sheet 13: 2001 Privacy Commissioner’s Approach to Promoting Compliance 317
Appendix 8321
Summary of complaint handling provisions, including powers to investigate .......... 321
Appendix 9326
Complaints Statistics ....................................................................................................... 326
Appendix 10 ....................................................................................................................... 335
Own Motion (section 40 (2)) power ................................................................................ 335
Appendix 11 ....................................................................................................................... 337
Current Powers to enforce determinations ..................................................................... 337
Appendix 12 ....................................................................................................................... 338
Decision Appeal Processes in comparable legislation .................................................. 338
Appendix 13 ....................................................................................................................... 340
Demographic information about complainants ........................................................... 340
Appendix 14 ....................................................................................................................... 342
Complainant and respondent satisfaction survey ......................................................... 342
Foreword

This report is the first major examination of how the laws governing the use of personal information by the private sector in Australia have worked in their first years of operation.

It has been a significant project for the Office and leadership team since last August. The project team was headed by Robin McKenzie.

The report has drawn on information and views from a wide range of sources including individuals, businesses, industry organisations, interest groups, and government agencies across the Commonwealth, and states and territories.

The review has benefited from discussions, consultations and material contained in submissions. I thank all those involved for contributing their ideas and views, and for the constructive way in which those views were conveyed.

I particularly thank the members of the Steering Committee and the Reference Group for their advice and guidance.

Many members of staff contributed in various ways – preparation of the Issues Paper, organising meetings for the Steering Committee and Reference Group, organising public consultations, analysing submissions, developing policy options, putting submissions on the website, undertaking surveys, writing sections of the report, editing and formatting. The Corporate and Public Affairs Section of the Office was involved in all aspects of the review process.

While I hesitate to single out individuals, it would be remiss if I did not acknowledge the major contributions of Robin McKenzie, Pauline Kearney, Paul Armstrong, Chris Cowper and Timothy Pilgrim. Suzanne Christian was responsible for the report compilation, formatting and editing.

To my staff, I express my gratitude for their contribution to this important review and I look forward to further improving the operation of the private sector provisions for the benefit of the community and business.

Karen Curtis
Privacy Commissioner

March 2005
Overview and Executive Summary

Approach to the review

Terms of reference

The Office has undertaken a review of the operation of the private sector provisions of the Privacy Act to see whether they meet their objectives. The objects are outlined in the terms of reference from the Attorney-General which are at Appendix 1.

Participants in the review

In the course of the review, information has been considered from a wide range of sources. They are:

- 136 written submissions
- 12 stakeholder workshops in all capital cities
- the Review Steering Committee, which includes members of the Privacy Advisory Committee
- the Review Reference group, which includes over 40 representatives from community, business and government
- the Office’s Community Attitudes Research
- research conducted by other stakeholders, for example, the National Health and Medical Research Council and the Australian Direct Marketing Association
- statistics collected by this Office either specifically for this review, or from its complaints management system
- Office staff experience in the course of providing policy advice to stakeholders, or managing complaints
- meetings with stakeholders.

A wide range of stakeholders have participated in the review. They include major business and industry sectors, including banking, insurance, finance, private detectives and debt collection, credit reporting, marketing, fundraising, health and allied care, manufacturing, retail, small business, housing, real estate, superannuation, internet, hospitality and welfare. There has also been input from consumer and privacy advocacy groups including consumer, credit, health and academia. In addition, the Office has received input from state and federal government agencies, including health, law enforcement agencies and other regulators, and also dispute resolution bodies.

Timing of the review

The private sector provisions have been in operation since 21 December 2001, or just over three years for non-small business operators, and since
21 December 2002, or just over two years for small businesses that do not qualify for the small business exemption. Given that implementing a privacy scheme, particularly for some sectors, involves complex attitude change and understanding rather than simply complying with clear, black letter law, this is a relatively short period of time to be assessing the operation of the provisions.

In addition, it was not possible to conduct the kind of detailed quantitative research that might give a clearer indication of the actual level of business compliance with its obligations under the scheme. Further, because the scheme is complaint based and the Office has only limited powers to investigate practices on its own initiative, it is possible that there are areas of non-compliance of which the Office is not aware. As a result, although the Office has sought to gain and draw upon quantitative evidence to the extent it is possible and available, it is in the end relying to a considerable extent on anecdotal evidence as well as its own complaint statistics for its conclusions.

**Provisions work well on balance**

**Overview**

The review process shows that the private sector provisions have met with their objectives in some areas and not in others. In some areas it has failed to meet with an objective, but in practice the impact may not have been significant. In others, objectives were met in a way quite different from that envisaged at the time the legislation was implemented. In some, the provisions have not met the objective.

Indeed, it could be argued for example that the private sector provisions have not met the two objectives of ‘a national scheme’ or ‘international concerns’. But this does not take away from the overall effect that the National Privacy Principles (NPPs) have worked well and delivered to individuals protection of personal and sensitive information in Australia in those areas covered by the Act.

**No fundamental flaw**

Although 85 recommendations have been made, this does not equate to dissatisfaction with the provisions. Rather, it means with the benefit of three years experience it has become apparent there are ways to improve existing elements of the regime, and there are external influences which have impacted on the efficacy of the legislation.

Although there were a few calls from privacy advocates for the Government to ‘go back to the drawing board’ entirely on the provisions, the Office has no
substantive evidence to suggest that the private sector scheme has any significant flaws to warrant dramatic changes.

**Provisions have generally worked well for business**

The overall view from the business sector is that the scheme has worked well for them, and that there is considerable support for it as it currently stands. Generally speaking, it appears that in most areas, the scheme has met its objective of not unduly impeding the free flow of information, or the right of business to achieve their objectives in an efficient way.

**Consumers are less satisfied**

Generally speaking however, those representing the consumer and privacy advocate groups were less satisfied that the private sector provisions had met their objectives of adequately providing for the privacy rights of individuals.

**International concerns**

One area where the private sector provisions have not met their objectives in the way that was anticipated is the objective of meeting international concerns and Australia’s international obligations relating to privacy. It appears that this has been less of a concern to many stakeholders than might have been expected at the time the provisions were enacted. A particular example of this is achieving European Union (EU) adequacy to enable businesses to engage in trade involving personal information with European businesses.

Despite the fact that the private sector provisions have not yet been found adequate by the EU, in general, business does not report a major impediment to trade. In addition, the issue of global trade beyond the EU has meant that the need to address consistency in privacy regulation at a global level has become important. The APEC initiatives on privacy are evidence of this shift.

**Approved NPP Codes**

Another area where the objectives of the private sector provisions have not been achieved in the way that was anticipated is the adoption of industry and organisation codes by the private sector to regulate their collection, use and disclosure of personal information. There are only three approved codes under the Privacy Act. However, there is no call for the repeal of the code provisions of the Act despite the very low level of take-up. Most businesses appear content to be regulated by the NPPs and to have the Office as their external complaints handling body.
A single national scheme

There is significant inconsistency

There is evidence that the failure of the privacy sector provisions to meet their objective of achieving national consistency in privacy regulation has had consequences for business efficiency. There is also some evidence that this has posed some impediments in the way of individuals seeking to be aware of, and have respected, their privacy rights. The inconsistency operates at a number of levels, including within the Privacy Act itself, within Commonwealth regulation impacting on privacy, and between state and Commonwealth legislation. The area of privacy involving health information, including health research has been clearly identified as being greatly affected by all these levels of inconsistency. Other areas affected include employee privacy and tenancy databases.

Reasons for the inconsistency

These inconsistencies have emerged for a number of reasons, some of which relate directly to the formulation of the private sector provisions. Others are a consequence of the rapidly changing environment in which the provisions are operating, and in particular, the heightened security concerns following September 11, and the developments in new technology.

One factor contributing to inconsistency is that within the Privacy Act, there are two sets of slightly different privacy principles, one for the Australian public sector and one for the private sector. As the Government has increasingly drawn upon the private sector - for example, welfare organisations - to carry out activities that were once performed by its agencies, this has become more of an issue.

Another factor appears to be the presence of exemptions in the Act. Submissions and consultations suggest that areas of inconsistency are arising because states and territories are legislating in areas covered by the exemptions. A key example of concern to business is the area of surveillance in the workplace. In the absence of privacy protection in this area in the federal Privacy Act, states and territories are legislating and each in a slightly different way.

There are also problem areas such as the regulation of tenancy databases by states and territories. As the NPPs do not totally regulate tenancy databases states and territories are legislating in this area, once again, in a slightly different way.

The desire for more detailed and binding guidance for health care providers together with inconsistency between private sector provisions and state public sector privacy principles, could also be considered reasons for states to
legislate in the health area. Submissions from business and consumers, and consultations indicate overwhelmingly that this has created a range of different rules that is confusing for health care providers, other businesses holding health information and consumers.

The Office’s complaints caseload that is larger than expected as a result of the private sector provisions has meant that the Office has not clarified the application of the NPPs in some of these areas (for example, tenancy databases) as speedily as it would like. In the mean time, states have moved to address what was emerging as a community need to ensure that tenants were not denied housing as a result of inaccurate and unfair listings.

Finally, rapidly changing technology has resulted in Commonwealth legislation that is outside of, but overlaps with, the Privacy Act. The Spam Act 2003 is an example. Spam was less of a concern in 1999 when the private sector provisions were formulated and the private sector provisions did not address this issue. This situation may arise again with the (future) development of new pervasive technologies. Businesses are concerned to ensure that when it does, the provisions fit well with the private sector provisions.

**Approach to recommendations**

This report makes a range of recommendations including strategies to address these inconsistencies. But as indicated by the complex factors contributing to these, there is no easy or single fix, especially in a federal system of government. Resolving the issues will involve commitment from all levels of government and a willingness to focus on the big picture.

One thing that became clear in conducting the review is that many of the issues that arise in relation to the operation of the private sector provisions are inter-related. This inter-relation has to be taken into account in recommendations. Recommendations on one aspect of operation will also have the potential to address issues on other aspects of operation.

It is also the case that there are a number of ways that issues arising out of the review could be addressed. Which approach is taken in one area, may affect what approach is best taken in other areas. For this reason, in a number of areas, this report has made recommendations as options that could be taken up depending on the approach taken in addressing other issues.

**Resourcing implications of reform**

In developing recommendations as part of this review, the Office has been aware of the resource implications of reform. Since the implementation of the private sector provisions, the Office has shifted resources from its guidance and advice role to its compliance role to try to better manage and resolve the complaints received. Even so, there is an unacceptably long waiting list of complaints to be handled. This satisfies neither business, who have invested
in compliance and in whose interest it is to have complaints against them settled quickly, nor consumers.

Submissions from all sectors discuss funding for the Office\(^1\). A number of submissions expressly support an increase in resources being granted to the Office\(^2\). Many of these submissions are particularly concerned by the backlog of complaints and subsequent delay in resolving complaints\(^3\).

There was also a general call for more resources to ensure consumers and businesses are educated about their rights and obligations under privacy laws.\(^4\)

In this review recommendations are made that, if implemented, will impact upon the operation of the Office. This has implications in terms of resources, for both staff and program delivery.

**Main recommendations**

This report makes recommendations about how the operation of the private sector provisions could be improved. Recommendations are primarily written as either actions that the Australian Government should consider doing, or as measures that the Office could or intends to undertake. A small number of recommendations involve measures that could be taken by state and territory governments.

Some recommendations involve broad high level principles around the operation of the private sector provisions, for example, recommendations to improve national consistency in privacy regulation, including health privacy regulation, and to ensure that the private sector provisions adequately protect privacy in the face of rapidly developing new technologies.

Recommendations for measures to raise awareness of both consumers and business on a range of topics are found in a number of places in the report. These particular recommendations could be regarded as forming the ‘lynch pin’ for a scheme that is intended to operate in a way that benefits individuals while recognising the right of businesses to achieve their objectives in an efficient way.

---

\(^1\) See for example ANZ 40, Business SA 92, Australian Medical Association 29, Australian Privacy Foundation 90, Baycorp Advantage 86, Consumer’s Federation of Australia 65, Consumer Credit Legal Centre (NSW) Inc 62, Coles Myer 60, Xamax 3, Australian Banker’s Association 70, Australian Finance Conference 63, Australian Consumers’ Association 15, Graham Greenleaf 47, Tenants Union of Qld Inc 69, Fundraising Institute of Australia Ltd 52.

\(^2\) 90, 86, 60, 63, 40.

\(^3\) For example 90, 29, 65, 62, 63, 15, 47, 69 The AMA submission says that a number of patients lodge privacy complaints with the AMA as well as the Office. The AMA suggests that this may be attributed to the Office being unable to respond in a timely or satisfactory manner.

\(^4\) 29, 65, 62, 60.
Other recommendations aim to increase the control that individuals have over their personal information, particularly in relation to information collected about them indirectly or used or disclosed for other purposes such as direct marketing. These include measures to promote short form privacy notices, and a general opt-out right for direct marketing.

The report makes recommendations about the small business exemption aimed at simplifying its application while suggesting that some sectors that have higher privacy risks should be covered by the private sector provisions.

The report also makes recommendations aimed at improving the transparency and fairness of the Office’s complaints process, and to enable it to better identify and address systemic issues.

Some issues raised are complex and need further consideration by the Australian community. The Office identified the application of the private sector provisions to research, in particular medical research, and to new technologies as warranting further debate. The main recommendations on these issues are that they should be considered in the context of a wider review of the Privacy Act.

In response to concerns that organisations need more guidance or that the NPPs may need amending to ensure that they are applied in a commonsense way, recommendations are made on such matters as alternative dispute resolution schemes, access to health records and major national emergencies.

The report makes a number of more technical recommendations that aim to increase certainty about the application of the NPPs, which in many cases clarify what is already existing practice.

Throughout the report, but particularly in the recommendations, there has been careful consideration of the balance between protecting individual rights while recognising the collective needs of the community including the business community.

Finally, it became apparent that while the private sector provisions work well, it may be appropriate for the Government to undertake a wider review of privacy for Australians in the 21st century.

The NPPs are based on principles developed in the 1970s and it may be fitting to consider how the operating environment has changed over the last 30 years. For example: Is our definition of personal information still appropriate given technological advances? Do we need different sets of privacy principles covering the private and public sectors? Should the legislation make a distinction between data controllers and data operators? Should the legislation only cover protection of data about living persons? In a changed security environment what are people’s expectations about their personal information?
In some of the 85 recommendations there is a reference to this wider review of privacy. Given that it is a recurring theme throughout the report to give more considered thought to ‘bigger picture’ issues, a recommendation has been made here in the Overview Section. It is the first recommendation listed below, and is followed by the recommendations as identified in each chapter.

**Recommendations:**

**Recommendation: Wider review of Privacy Act**

1. The Australian Government should consider undertaking a wider review of privacy laws in Australia to ensure that in the 21st century the legislation best serves the needs of Australia.

**Recommendations: National consistency**

The Privacy Act has not achieved its object of establishing a ‘single comprehensive national scheme’ for the protection of personal information. As submissions reveal, national consistency is important to business, to charities and to individuals. The lack of national consistency contributes significantly to the costs imposed on business.

2. The Australian Government should consider amending section 3 of the Privacy Act to remove any ambiguity as to the regulatory intent of the private sector provisions.

3. The Australian Government should consider asking the Council of Australian Governments (COAG) to endorse national consistency in all privacy related legislation.

4. The Australian Government should consider setting in place mechanisms to address inconsistencies that have come about, or will come about, as a result of exemptions in the Privacy Act, for example, in the area of workplace surveillance.

5. The Australian Government should consider commissioning a systematic examination of both the IPPs and the NPPs with a view to developing a single set of principles that would apply to both Australian Government agencies and private sector organisations. This would address the issues surrounding Australian Government contractors.

6. The Australian Government should consider changing, by legislative amendment, the name of the Office of the Privacy Commissioner to the Australian Privacy Commission.

7. The Australian Government should consider amending the Privacy Act to provide for a power to make binding codes.
Recommendations: Telecommunications consistency

8  The Australian Government should consider amending the Privacy Act and the Telecommunications Act to clarify what constitutes authorised uses and disclosures under the two Acts, and to ensure that the Privacy Act cannot be used to lower the standard of privacy protection in the Telecommunications Act.

9  The Australian Government should consider making regulations under section 6E of the Privacy Act to ensure that the Privacy Act applies to all small businesses in the telecommunications sector, including Internet Service Providers and Public Number Directory Producers.

10 The Office will discuss with the Australian Communications Authority the development of guidance to clarify the relationship between the private sector provisions of the Privacy Act and Part 13 of the Telecommunications Act.

11 The Office will discuss with the Australian Communications Authority the development of guidance to clarify the relationship between the private sector provisions of the Privacy Act and the Spam Act.

Recommendations: Health consistency

12 The Office urges the National Health Ministers’ Council to finalise the National Health Privacy Code. This should include agreement by all jurisdictions on the contents of the code and on its consistent implementation in each jurisdiction.

13 The Australian Government should consider adopting the National Health Privacy Code as a schedule to the Privacy Act. This would recognise the Australian Government’s part in the consistent enabling of the Code. Should agreement not be reached by all jurisdictions about implementing the Code, the Australian Government should still consider adopting the code as a schedule to the Act to provide greater consistency of regulation for the handling of health information by Australian Government agencies and the private sector. (See also recommendations 29, 33 and 35.)

Recommendations: Residential tenancy databases

14 The Australian Government should advance as a high priority the work currently being undertaken by the Working Group on Residential Tenancy Databases of the Ministerial Council on Consumer Affairs/Standing Committee of Attorneys-General.
15 The Australian Government should consider, depending on the outcome of the Ministerial Council on Consumer Affairs/Standing Committee of Attorneys-General, making the Privacy Act apply to all residential tenancy databases. This could be done by using the existing power under section 6E to prescribe them by regulation, or by amending the consent provisions (section 6D(7) and section 6D(8)) that apply to the small business exemption. (See recommendation 53.)

16 If the Privacy Act is amended to provide for a power to make a binding code, (see recommendation 7), and depending on the outcome of the Ministerial Council on Consumer Affairs/Standing Committee of Attorneys-General, the Privacy Commissioner could make a binding code that applies to tenancy databases.

**Recommendation: EU ‘adequacy’ and APEC**

17 There is no evidence of a broad business push for ‘adequacy’. Given the increasing globalisation of information, however, there may be long term benefits for Australia in achieving EU ‘adequacy’. Certainly the globalisation of information makes the implementation of frameworks such as APEC important. The Australian Government should continue to work with the European Union on the ‘adequacy’ of the Privacy Act and to continue work within APEC to implement the APEC Privacy Framework.

**Recommendation: NPP 9**

18 The Office will provide further guidance to assist organisations comply with NPP 9 by issuing an information sheet outlining the issues that should be addressed as part of a contractual agreement and how to more easily assess whether a privacy regime is substantially similar.

**Recommendations: Control over personal information**

19 The Australian Government should consider amending NPP 5.1 to provide for short form privacy notices. This could also clarify the obligations on organisations to provide notice, and to clarify the links between NPP1.3 and NPP 5.1.

20 The Office will encourage the development of short form privacy notices. It will also play a more active role in assisting businesses develop their notices by developing template notices for different sectors, in consultation with them, and by issuing example of both satisfactory and unsatisfactory notices.
21 The Office will develop guidance to the effect that privacy notices should be dated.

22 The Office will develop guidance on bundled consent, noting the possible tension between the desirability of short form privacy notices and the desirability of lessening the incidence of bundled consent.

Recommendations: Direct marketing

23 The Australian Government should consider amending the Privacy Act to provide that consumers have a general right to opt-out of direct marketing approaches at any time. Organisations should be required to comply with the request within a specified time after receiving the request.

24 The Australian Government should consider amending the Privacy Act to require organisations to take reasonable steps, on request, to advise an individual where it acquired the individual’s personal information.

25 The Australian Government should consider exploring options for establishing a national ‘Do Not Contact’ register.

Recommendations: Consumer education

26 The Australian Government should consider specifically funding the Office to undertake a systematic and comprehensive education program to raise community awareness of privacy rights and obligations.

27 The Office will continue to collect demographic information about complainants. It will seek to identify and then remove any barriers that prevent sectors of the community from knowing about and exercising their privacy rights.

Recommendations: Access generally

28 The Australian Government should consider amending NPP 6 to provide that when an individual’s personal information is corrected in response to a request from the individual, the organisation should be obliged to notify third parties, where practicable, that they have received the inaccurate information.

29 The Australian Government should consider adopting the Australian Health Ministers’ Advisory Council (AHMAC) Code as a schedule to the Privacy Act (see recommendation 13). This will address the issue of intermediaries, and the issue of fees for access. (See also recommendations 13, 33 and 35.)
30 The Office will develop further guidance on the operation of NPP 6.1 on ‘serious threat to life or health’, explaining that a serious threat to a therapeutic relationship could be a serious threat to a person’s health. This will go some way towards addressing what appears to be a too narrow interpretation of NPP 6.1(b) by some practitioners.

31 The Office will develop guidance on fees for access to personal information.

32 The Office will develop guidance on the meaning of NPP 6.5 which requires than an individual ‘establish’ that information is not accurate before the organisation need to take reasonable steps to correct it.

Recommendations: Transfer of health records

33 The Australian Government should consider adopting the Australian Health Ministers’ Advisory Council (AHMAC) code as a schedule to the Privacy Act. This will address the issue of the transfer of health records to another health service provider. (See also recommendations 13, 29 and 35.)

34 The Australian Government should consider, if the AHMAC Code is not adopted into the Privacy Act, amending the NPPs to include a new principle along the lines of National Health Privacy Principle 11 in the AHMAC Code.

Recommendations: Health service ceases to operate

35 The Australian Government should consider adopting the AHMAC code as a schedule to the Privacy Act. This will address the issue of access to health records when a health service ceases to operate. (See also recommendations 13, 29 and 33.)

36 The Australian Government should consider, if the AHMAC Code is not adopted into the Privacy Act, amending the NPPs to include a new principle along the lines of National Health Privacy Principle 10 in the AHMAC Code.
Recommendations: Complaints handling and compliance

Approach to compliance

37 The Office will maintain its current approach to compliance including the focus on attempting to conciliate complaints in the first instance as set out in Information Sheet 13. However, the Office will consider whether it might be appropriate in some circumstances to use its other powers earlier, such as the determination making power.

38 The Office will consider options for providing more feedback on systemic issues either in advice or guidance or in some form of regular update to stakeholders.

39 The Office will consider promoting privacy audits by private sector organisations, including by providing information on the value of auditing as evidence of compliance in the event of complaints and by developing and providing privacy audit training for organisations.

Review rights for complaint decisions

40 The Australian Government should consider amending the Privacy Act to give complainants and respondents a right to have the merits of complaints decisions made by the Privacy Commissioner reviewed.

Fair and transparent complaint processes and resolution

41 The Australian Government should consider amending National Privacy Principle 1.3 to require organisations to tell individuals how they can complain to the organisation; and that, if the complaint is not resolved, they can also complain to the Privacy Commissioner or (where relevant) the code adjudicator.

42 The Office will review its complaints handling processes and will consider the circumstances in which it might be appropriate to make greater use of the Commissioner’s power to make determinations under section 52 of the Privacy Act.

43 The Office will also consider measures to increase the transparency of its complaints processes and complaint outcomes.
Additional powers

44 The Australian Government should consider amending the Privacy Act to:

- expand the remedies available following a determination under section 52 to include giving the Privacy Commissioner power to require a respondent to take steps to prevent future harm arising from systemic issues
- provide for enforceable remedies following own motion investigations where the Commissioner finds a breach of the NPPs
- provide a power for the development of binding codes and/or binding guidelines in cases where there is a strong public interest, where more detailed guidance is warranted or complaints reveal recurrent breaches (see recommendation 7).

Resourcing implications and complaint handling

45 The Australian Government should consider the strong calls by a wide range of stakeholders for the Office to be adequately resourced to meet its complaint handling functions.

46 The Australian Government should consider amending the Privacy Act to give the Commissioner a further discretion not to investigate complaints where the harm to individuals is minimal and there is no public interest in pursuing the matter.

Recommendation: Approved privacy codes

47 The Office will review the Code Development Guidelines dealing with the processes relating to code approval with a view to simplifying them.

Recommendations: Business awareness

48 The Australian Government should consider the benefits of greater business and community awareness of privacy and specifically fund the Office to undertake a systematic and comprehensive education program to raise business awareness.

49 The Office will review existing information sheets and develop information sheets on key issues identified in submissions.

50 The Office will develop strategies for communication with stakeholders, including establishing a privacy contact officer network for private sector organisations.
Recommendations: Small business exemption

51 The Australian Government should consider retaining but modifying the small business exemption by amending the Privacy Act so that the definition of small business is to be expressed in terms of the ABS definition, currently 20 employees or fewer, rather than annual turnover.

52 The Attorney-General should consider using the power to prescribe under section 6(E) of the Privacy Act, the tenancy databases and telecommunications sectors including Internet Service Providers and Public Number Directory Producers as businesses to be covered by the Act. (See recommendations 9 and 15.)

53 The Australian Government should consider amending the Privacy Act to remove the consent provisions (sections 6D(7) and 6D(8)).

Recommendations: Private sector contracting

54 The Australian Government should consider amending NPP 4 to impose an obligation on an organisation to ensure personal information it discloses to a contractor is protected.

55 The Australian Government should consider, in the context of the wider review of the Privacy Act, (see recommendation 1) whether there should be a distinction between data controllers and data operators.

56 The Office will amend the Guidelines to the National Privacy Principles to clarify that businesses that give personal information to contractors for the purpose of performing a function on their behalf should impose contractual obligations on the contractor to take reasonable steps to protect the information.

Recommendation: Due diligence

57 The Australian Government should consider amending the NPPs to take into account the practice of due diligence.

Recommendations: Media exemption

58 The Australian Government should consider amending the Privacy Act so that:

- the Australian Broadcasting Authority (ABA) and media bodies must consult with the Privacy Commissioner when developing codes that deal with privacy and
• the term ‘in the course of journalism’ is defined and the term ‘media organisation’ is clarified.

59 The Office will, in conjunction with the ABA, provide greater guidance to media organisations as to appropriate levels of privacy protection, especially in relation to health issues, and make organisations aware that the media exemption is not a blanket exemption.

Recommendations: Research

60 As part of a broader inquiry into the Privacy Act (see recommendation 1), the Australian Government should consider:

• how to achieve greater consistency in regulating research activities under the Privacy Act
• whether regulatory reform is needed to address the issue of de-identification in the context of research and the handling of health information
• where the balance lies between the public interest in comprehensive research that provides overall benefits to the community, and the public interest in protecting individuals' privacy (including individuals having choices about the use of their information for such research purposes)
• whether there is a need to amend NPP 2 to permit the use and disclosure of personal information for research that does not involve health information
• undertaking further research and education work with the broader community to ensure that the balance between research and privacy accords with what the community expects and understands.

61 The Office will issue guidance in relation to NPP 2 to clarify that organisations can disclose health information for the management, funding and monitoring of a health service.

62 The Office will work with the National Health and Medical Research Council to simplify the reporting process for human research ethics committees under the section 95A guidelines.

Recommendations: Decision-making where capacity is impaired

63 The Australian Government should consider, in order to ensure that the Privacy Act does not prevent individuals with a decision-making disability from receiving a range of utilities and other services, amending NPP 2 to permit the disclosure of non-health information to a class of persons the same, or similar, to that described in NPP 2.5,
where an organisation considers the disclosure to be necessary for the management of the person’s affairs in a way that their financial or other interests are secured or safeguarded.

It would be appropriate to consider developing such an amendment in consultation with the Australian Guardianship and Administration Committee.

64 The Office will, in recognition that disclosures of health information under NPP 2 are appropriately permitted in law but may not occur in practice, develop further and more practical guidance.

**Recommendation: Law enforcement**

65 The Office will work with the law enforcement community, private sector bodies and community representatives to develop more practical guidance to assist private sector organisations to better understand their obligations under the Privacy Act in the context of law enforcement activities.

**Recommendation: Private investigations**

66 The Australian Government, through the Attorney-General, should consider requesting that the Standing Committee of Attorneys General (SCAG) consider the issues raised by the Australian Institute of Private Detectives as they are broader than the Privacy Act.

**Recommendations: Alternative dispute resolution schemes**

67 The Australian Government, in recognising the important role played by Alternative Dispute Resolution (ADR) schemes, and in an attempt to formalise advice already given by the Office, should consider:

- amending NPP 2 to enable use and disclosure of personal information to ADR schemes in the course of handling disputes
- amending NPP 10 to enable collection of sensitive information where it is necessary for the investigation and resolution of claims under an ADR scheme
- defining the term ‘Alternative Dispute Resolution Scheme’ for these purposes in the Act.
Recommendations: Large scale emergencies

68 Privacy laws should take a common sense approach. There needs to be an appropriate balance between the desirability of having a flow of information and protecting individual’s right to privacy. In developing an exception to disclosure for cases of national emergencies, consideration should be given to the seriousness of the privacy breach versus that of protecting privacy.

In large scale emergencies, the consequences of disclosure should be compared to the consequences of non-disclosure. Consideration also needs to be given to the potential identity fraud that may occur during such a time, especially if disclosure is allowed to the media.

The Australian Government should consider:

- amending NPP 2 to enable disclosure of personal information in times of national emergency to a ‘person responsible’
- extending the NPP 2.5 definition of ‘person responsible’ to include a person nominated by the family to act on behalf of the family
- amending the Privacy Act to enable the Privacy Commissioner to make a Temporary Public Interest Determination without requiring an application from an organisation
- defining ‘National Emergency’ as ‘incidents’ determined by the Minister under section 23YUF of the Crimes Act 1914.

Recommendations: New technologies

69 The Australian Government should consider, in the context of a wider review of the Privacy Act (see recommendation 1) reviewing the National Privacy Principles and the definition of personal information to assess whether they remain relevant in the light of technological developments since the OECD principles were developed. This should ensure that the private sector provisions remain technologically neutral and relevant to protect data privacy in the main contexts in which information about people is currently collected, used and disclosed.

70 The Australian Government should consider initiating discussions through appropriate international forums about how to deal with major international jurisdictional issues arising from global reach of new technologies such as Voice over Internet Protocol (VoIP).

71 The Australian Government should consider developing specific enabling legislation to underpin any national electronic health records system. The legislation should be consistent with the National Health Privacy Code, but also include enhancing protections for matters such as the voluntariness of the system and limitations upon the uses of people’s health records.
The Office will issue further guidance, consistent with the current law, on what is personal information which takes into account the fact that in the current environment it is more difficult to assume that any information about people cannot be connected.

The Office could use, if necessary, any new powers to develop binding codes (see recommendation 7) to deal with technologically specific situations.

**Recommendation: NPP 1.3(d)**

The Australian Government should consider amending NPP 1.3(d) to make clear that an organisation collecting personal information from an individual must take reasonable steps to notify them of likely disclosures generally, including to public sector agencies of the Australian Government, state or local governments, other bodies and private individuals.

**Recommendation: Reasonable steps for NPP 1.3 and 1.5**

The Australian Government should consider amending NPP 1.3 and NPP 1.5 to make clear that there are situations in which the reasonable steps an organisation might take to provide notice to an individual may equate to no steps.

**Recommendation: NPP 1.5 – ‘Someone’**

The Australian Government should consider amending NPP 1.5 to remove the term ‘someone’, and to make clear that an organisation has an obligation to take reasonable steps to provide notice to an individual when collecting their personal information indirectly, from any source.
**Recommendations: Primary purpose and health information**

77 The Office will work with the health sector to develop further guidance about the operation of NPP 2 as it specifically relates to the issue of primary and secondary purpose in health care.

78 The Office will provide clearer guidance on the operation of NPP 2 to give more effective and practical assistance to demonstrate how the principle operates. This will take into account the range of relationships between health services and individuals, particularly where individuals agree to a holistic approach to the delivery of a health service.

**Recommendation: NPP 3 - Data quality**

79 The Office will provide further guidance to organisations about their obligations under NPP 3, particularly to ensure they take a proportional approach to complying with the principle. This will include guidance about organisations taking into account whether or not there are good privacy reasons for seeking to update an individual's personal information.

**Recommendation: NPP 7 - Identifiers**

80 The Australian Government should consider using the existing regulation-making mechanism under NPP 7 to address circumstances such as those identified by Centrelink regarding concessional entitlements.

**Recommendations: NPP 10 - Public Interest Determinations**

81 The Australian Government should consider amending NPP 10 to include an exception that mirrors the operation of Public Interest Determinations 9 and 9A.

82 The Australian Government should consider undertaking consultation on limited exceptions or variations to the collection of family, social and medical history information, particularly with regard to genetic information and the collection practices of the insurance industry.
Recommendations: NPP 10.2(b)

83 The Australian Government should consider amending NPP 10.2 to permit the collection of health information (under NPP 10.2(b)(i)) ‘as authorised by law’ in addition to ‘as required by law’.

84 The Australian Government should consider amending NPP 10.2(b)(ii) to clarify the nature of the binding rules intended to be covered by this provision, particularly with regard to the substantive content of such rules.

Recommendations: Deceased persons

85 If the National Health Privacy Code is adopted into the Privacy Act (see recommendation 13), then protection for health information under these provisions would extend to deceased persons. Also, the Australian Government’s response to the Australian Law Reform Commission and the Australian Health Ethics Committee’s inquiry into the protection of human genetic information in Australia may have implications for the Privacy Act. In addition, the Australian Government should consider as part of a wider review (recommendation 1) whether the jurisdiction of the Privacy Act should be extended to cover the personal information of deceased persons.
1 Background

1.1 This Inquiry

Background to the review

The Review of the Privacy Act was foreshadowed by the former Attorney-General the Hon Daryl Williams AM QC MP in his second reading speech for the Privacy Amendment (Private Sector) Act 2000. The Commissioner was asked to review the operation of the private sector provisions of the Act by the Attorney-General, the Hon Philip Ruddock MP, on 13 August 2004.

Terms of Reference

The Office conducted the review within the terms of reference outlined by the Attorney-General. They are included in full at Appendix 1 of this report. They provide for an assessment of the operation of the private sector provisions and a consideration of the extent to which the private sector provisions meet their objects. These objects include creating a single comprehensive national scheme for the appropriate handling of an individual’s personal information by organisations, in a way that:

- meets international concerns and obligations relating to privacy
- recognises individuals’ interests in protecting privacy and
- recognises important human rights and social interests that compete with privacy, including the general desirability of the free flow of information (through the media and otherwise) and the right of business to achieve its objectives efficiently.

Matters not included in the review

The terms of reference exclude aspects of the private sector provisions from the review including:

- genetic information
- employee records
- children’s privacy and
- electoral roll information and the related exemption of political organisations from the Privacy Act.

The terms of reference state that these areas are currently, or have recently been subject to processes of review.
The terms also mean that Part IIIA of the Privacy Act, which deals with credit reporting has not been reviewed. However the credit reporting provisions where relevant to the operation of the private sector provisions have been considered.

**Other relevant privacy related reviews and processes**

There are a number of processes underway that touch on privacy in some way. For example, initiatives to develop a national health code (Australian Health Ministers’ Advisory Council (AHMAC) process) and the review of privacy protection for employee records. In developing the recommendations in this report, the Office has taken into account, where appropriate, the work being done in these areas.

**Research**

To help inform the review work, including submissions to the review, the Office conducted research into community attitudes towards privacy in April 2004. This complements research it conducted in July 2001 into attitudes towards privacy in the spheres of government, business and the community. This Community Attitudes Research can be found on the Office’s website. The results of the 2004 research are summarised at Appendix 6 and the full report is to be found on the Office’s web site.

**Framework for assessing issues**

The terms of reference ask the Privacy Commissioner to consider the degree to which the private sector provisions meet their objects. The Office used this framework for assessing the provisions. This involved considering the following issues.

1. Do the provisions provide a comprehensive, national, consistent set of standards for privacy? Do they fit seamlessly into the Privacy Act? Do they relate effectively with other federal privacy provisions, the privacy laws of the States and Territories and other relevant federal law?

2. Do the provisions operate in a way that assists Australian businesses to operate internationally? Are they adequate to ensure Australia fulfils its international obligations relating to privacy?

3. Are individuals confident that their interests in protecting their privacy are recognised and that personal information that is collected, used, stored and disclosed by organisations is adequately protected? Are individuals aware of, and able to exercise, their rights?
4. Do the provisions strike an appropriate balance between privacy and competing human rights and social interests, including free speech, medical research, national security, law enforcement and property rights? Is there a free flow of information? Is business aware of its obligations and able to comply with them while still achieving its objectives efficiently?

**Conduct of the review - overview of consultation**

The Privacy Commissioner received the terms of reference from the Attorney-General on the 13 August 2004. The review of the private sector provisions was completed by 31 March 2005. The Privacy Commissioner encouraged widespread public participation in the review through a number of measures. The Office:

- made three media releases in August, September and October advertising the review, asking organisations and individuals to give their views about the operation of the private sector provisions and informing the public about key dates in the conduct of the review
- contacted stakeholders listed on the Office’s contacts database and network list via e-mail about the review requesting submissions and promoting the public consultation forums. The Office made follow up phone calls to stakeholders preceding their local public consultation forum.
- circulated an e-mail notification about the review through relevant industry and government networks
- gave a number of presentations to industry forums and national conferences
- conducted a number of private meetings with stakeholders at their request regarding the review and the operation of the private sector provisions of the Act.

The Commissioner appointed a steering committee to assist with and advise on the conduct of the review. The Steering Committee members were:

- **Charles Britton**, Senior Policy Officer, Information Technology and Communications, Australian Consumers' Association
- **Peter Coroneos**, Chief Executive Officer, Internet Industry Association
- **Ian Gilbert**, Director of Retail Regulatory Policy, Australian Bankers' Association
- **Graeme Innes**, Deputy Discrimination Commissioner, Human Rights and Equal Opportunity Commission
- **John O'Brien**, Senior Lecturer in Industrial Relations and Organisational Behaviour, University of New South Wales
- **Joan Sheedy**, Assistant Secretary, Information Law Branch, Attorney General's Department.

The Steering Committee met on five separate occasions throughout the process to discuss the conduct of the review.
The Commissioner also reconvened the core consultative group which had been formed by the Attorney-General in 1998 to advise on the development of the private sector provisions. The group, reconvened by the Commissioner and renamed the Review Reference Group, consisted of approximately 40 representatives from consumers groups, industry and government who have been affected by the operation of the Act. Approximately half of the reconvened group were part of the original group that advised on the introduction of the private sector provisions. The Review Reference Group was consulted regarding the conduct of the review, the issues contained in the issues paper, and the options for reform. The list of members is available at Appendix 2.

**Issues Paper**

To assist stakeholders to make submissions the Commissioner released an issues paper on 27 October 2004.

The issues paper sought to provide a framework for assessing the extent to which the private sector provisions met their objectives as defined in the terms of reference. The issues paper closely followed the terms of reference and sought to help stakeholders assess whether the provisions meet international concerns and Australia’s obligations relating to privacy. It raised issues about whether the legislation provides appropriate protection of individuals’ privacy while allowing a balance to be struck with competing human rights and social interests including the desirability of a free flow of information and the right of business to achieve its objectives efficiently.

**Consultation Meetings**

The Office organised consultation meetings in all of the capital cities during 2004. Meetings were held in:

- Adelaide on 4 November
- Perth on 11 November
- Hobart on 17 November
- Melbourne on 18 November
- Sydney on 22 November
- Darwin on 25 November
- Brisbane on 30 November
- Canberra on 8 December

There were also health forums held in Perth on 11 November, Melbourne on 18 November and Darwin on 25 November. In addition, a telecommunications forum was convened in Melbourne on 19 November 2004.

At each meeting the Commissioner or a representative of the Office led the discussion using a presentation which can be found on the Office’s website.
The consultation forums were attended by a wide range of participants from diverse industry sectors including the finance sector, direct marketing, credit reporting, debt collection, law firms, law societies, telecommunications, retail, real estate, fundraising and the health sector including, doctors, researchers and pharmacists, and the community sector including consumer and public interest advocates, community legal and tenancy advice centres and union representatives.

Issues raised in theses forums have been incorporated throughout this report.

**Written Submissions**

The Commissioner encouraged stakeholders to make written submissions to aid the Review. In all the Review received 136 written submissions (see Appendix 3) ranging in length and style from individuals, organisations, industry bodies, advocacy groups and government agencies. Of these, 20 submissions requested to remain confidential. These submissions can be found on the Office’s website.

**Structure of report**

The structure of this Report reflects the Terms of Reference received from the Attorney-General.

Chapter 1 gives background to the inquiry and an overview of the private sector provisions of the Privacy Act.

Chapter 2 examines the degree to which the private sector provisions establish national consistency in the way private sector organisations collect, hold, use, correct, disclose and transfer personal information.

Chapter 3 considers how adequately the private sector provisions meet international concerns and Australia’s international obligations relating to privacy.

Chapter 4 considers the effectiveness of the private sector provisions in protecting individuals’ rights to privacy.

Chapter 5 considers the effectiveness of the private sector provisions in enforcing individual rights to privacy.

Chapter 6 considers how effectively the private sector provisions balance an individual’s right to privacy with other competing social interests such as business efficiency and the desirability of a free flow of information.

Chapter 7 considers other social interests that compete with privacy and whether the private sector provisions have achieved the appropriate balance.

Chapter 8 looks at developments in new technologies.
Chapter 9 looks at whether any NPPs not addressed elsewhere in the report may need to be amended to create greater certainty in their interpretation.

Chapter 10 covers other issues that arise in relation to the private sector provisions.

### 1.2 Private Sector Provisions of the Privacy Act

#### History of Commonwealth Privacy Legislation

**Commonwealth agencies**

The Privacy Act was enacted in 1988. It provides for the Office of the Privacy Commissioner and a Privacy Commissioner and lists 11 principles governing the collection, use, storage, access to, maintenance and disclosure of an individual’s personal information. These Information Privacy Principles (IPPs) apply to personal information held by Australian Government agencies. Since 1994, the IPPs have also applied to Australian Capital Territory (ACT) agencies.

**Tax file numbers and credit reporting**

The Privacy Act also provides for the Commissioner to issue tax file number guidelines and to investigate acts or practices of tax file number recipients that breach these guidelines.

In 1990, the Privacy Act was amended to regulate the handling of credit reports and other credit worthiness information about individuals held by credit reporting agencies and credit providers.\(^5\)

**Private sector**

**Voluntary principles**

In February 1998, following extensive consultation, the Privacy Commissioner issued the National Principles for the Fair Handling of Personal Information (the National Principles), compliance with which was voluntary. This was partly in response to a directive on information privacy adopted in October 1995 by the European Parliament and the Council of the European Union (EU) which included a provision that personal data could not be transferred from an EU country to a non-EU country unless there was an adequate level of information privacy.

---

\(^5\) Privacy Act Part IIIA, Privacy Act 1988
Privacy Amendment (Private Sector) Act 2000

In late 1998, the Government announced its intention to legislate to support and strengthen privacy protection in the private sector. After widespread consultation the Privacy Amendment (Private Sector) Act 2000 was passed in December 2000 with a commencement date of 21 December 2001. It aimed to establish a single comprehensive national scheme governing the collection, holding, use, correction, disclosure and transfer of personal information by private sector organisations. It did so by means of the National Privacy Principles (NPPs) and provisions allowing organisations to adopt approved privacy codes.

Co-regulation

The approach adopted by the legislation was one of co-regulation. This refers to a legislative framework within which self regulatory codes of practice can be given official recognition. The aim of the legislation was 'to encourage private sector organisations and industries which handle personal information to develop privacy codes of practice'. In the absence of a code, the NPPs would apply. This co-regulation aimed to ensure consistency and standardisation of personal information handling.

Balancing rights and obligations

The legislation acknowledges that privacy is not an absolute right and that an individual’s right to protect his or her privacy must be balanced against a range of other community and business interests. These include the general desirability of a free flow of information (through the media and otherwise) and the right of business to achieve its objectives efficiently. The legislation seeks to achieve the appropriate balance by providing for, among other things, a number of exemptions from the legislative requirements, including most small businesses.

Key drivers for private sector provisions

The Explanatory Memorandum for the private sector provisions outlined concerns raised in consultations on the absence of privacy protection that self-regulation had not resolved. It said:

‘These concerns include

- the potential for barriers to international trade for business
- the lack of protection afforded to the consumer

---

6 Privacy Amendment (Private Sector) Bill 2000 Revised Explanatory Memorandum – Senate, November 2000, p 17.
7 Privacy Amendment (Private Sector) Bill 2000 Second Reading Speech, 12 April, House of Representatives Hansard p 15750.
8 Privacy Amendment (Private Sector) Bill 2000 Revised Explanatory Memorandum – Senate, November 2000, p17.
• the effects on the take-up of electronic commerce resulting from lack of protection to consumers
• the lack of comprehensive coverage of business
• the possibility that some States and Territories will impose stricter controls, which may result in inconsistencies between jurisdictions\(^9\).

Another factor underpinning the legislation was the International Covenant on Civil and Political Rights (ICCPR) that Australia had ratified. This provides that individuals shall not be subjected to arbitrary or unlawful interference with their privacy and that they have the right to the protection of the law against such interference or attacks\(^10\).

2004 amendments to the legislation

Amendments to the legislation in April 2004\(^11\) make it clear that the protection provided by NPP 9, which regulates transborder data flows, applies equally to the personal information of individuals who are Australian and those who are not. They remove the nationality and residency limitations on the power of the Privacy Commissioner to investigate complaints relating to the correction of personal information. They also give businesses and industries more flexibility in developing privacy codes by allowing the codes to cover otherwise exempt acts and practices where the authors of the code wish to do so.

What do the Private Sector Provisions cover?

Purpose

The private sector provisions of the Privacy Act give individuals control over the way personal information about them is handled by private sector organisations. They regulate the way many private sector organisations collect, use, keep secure and disclose personal information. They also give individuals a right to know what information an organisation holds about them and a right to correct it if it is wrong.

Who is covered?

The provisions apply to organisations, including corporations and unincorporated associations, with an annual turnover of more than $3 million.

They also apply, regardless of annual turnover, to all private sector health service providers, to organisations that buy and sell information without the individual's consent, and contracted Commonwealth service providers in relation to their contractual activities\(^12\). Specified acts and practices of

---

9 Privacy Amendment (Private Sector) Bill 2000 Revised Explanatory Memorandum – Senate, November 2000, p 11.
10 Article 17. Australia ratified the ICCPR on 13 August 1980.
12 Privacy Act Section 6D.
organisations are exempt from the operation of the Privacy Act. These include in general terms acts or practices:

- done by an individual other than in the course of the individual’s business, for example, in the course of his or her personal, family or household affairs \(^{13}\)
- that are related to an employee record and directly related to the employment relationship \(^{14}\)
- done in the course of journalism by a media organisation that is publicly committed to observing published privacy standards \(^{15}\) and
- done by a politician or political organisation, and their contractors, subcontractors and volunteers, in relation to electoral matters \(^{16}\).

**What obligations are imposed?**

In general terms, a private sector organisation covered by the Act must not do anything that breaches an approved code binding on it. If not bound by an approved code, it must not do anything that breaches an NPP.

**National Privacy Principles**

The NPPs govern the collection, use and disclosure, security, quality and access to and correction of personal information. They include principles applicable to the use and disclosure of personal information for specific purposes, including:

- direct marketing
- in the case of health information, research or statistical compilation or analysis relevant to public health or public safety
- protection of health and safety and
- law enforcement.

The general principle that a person should have access to information organisations hold about them includes exceptions, such as exceptions based on health and safety, law enforcement and national security. Special provisions apply to sensitive information, including information about an individual’s racial or ethnic origin, membership of political or professional or trade associations, religious beliefs and so on. Generally speaking, a higher level of protection is afforded sensitive information than personal information.

**Advice and guidance**

The Office plays an active role in raising awareness about individuals’ privacy rights and in addressing providing advice to business about its obligations. It provides information by way of its information hotline and its web site. The

---

\(^{13}\) Privacy Act Section 7B(1).
\(^{14}\) Privacy Act Section 7B(3).
\(^{15}\) Privacy Act Section 7B(4).
\(^{16}\) Privacy Act Section 7C.
web site contains all the Office’s publications, answers to Frequently Asked Questions, media comments, media releases, speeches, case notes, an online complaint checker, multi-lingual web pages, guidelines, information sheets, brochures and the annual report. Members of the Office also make speeches and presentations at a range of events.

Approved Codes

The Act provides for the approval of privacy codes by the Commissioner. To be approved a code must:

• set out obligations that, overall, are at least the equivalent of all the obligations set out in the NPPs
• specify which organisations are bound by the code
• bind only organisations that consent to be bound and
• if the code includes procedures for dealing with complaints, the procedures must meet specified standards.

In addition, members of the public must have been given adequate opportunity to comment on a draft of the code\(^{17}\). The Commissioner must keep a register of approved privacy codes\(^ {18}\).

Complaints

An individual may complain to the Commissioner about an interference with his or her privacy, unless an approved code applies and the code has its own code adjudicator. The Commissioner is required to investigate complaints, unless it is appropriate to exercise one of the discretions not to investigate, including for example, if the individual has not first complained to the organisation in question. If the complaint is upheld, the Commissioner may make a determination that the organisation should not repeat the conduct complained about.

\(^{17}\) Privacy Act Section 18BB.
\(^{18}\) Privacy Act Section 18BG.
2 National Consistency

2.1 National consistency overall

National consistency was goal of legislation

In introducing the private sector provisions of the Privacy Act, the then Attorney-General, the Hon Daryl Williams AM QC MP, noted that although some Australian businesses had already established privacy codes of practice this was not being done consistently. By contrast, the private sector amendments provide ‘a national, consistent and clear set of standards to encourage and support good privacy practices’. It was the Government’s intention:

‘to establish a single national comprehensive scheme for the protection of personal information by the private sector. However, state and territory laws would continue to operate to the extent that they are not directly inconsistent with the terms of the bill’¹⁹.

Issues

The issues paper suggested a number of topics for submissions related to national consistency. It asked:

- whether national consistency was important and whether or not it was being achieved
- about areas of overlap, including overlap between the private sector provisions and other laws or regulatory schemes and jurisdictional overlap
- about lack of clarity as a possible issue and
- about areas that are unregulated or under-regulated by the private sector provisions or other laws, and areas that are over-regulated.

The issues paper also suggested a number of topics for submission focussed on the Privacy Act itself. It asked about:

- issues arising from differences between the NPPs and IPPs
- the workability of the Australian Government contractor provisions, especially for contractors that would otherwise be exempt as a small business, and whether they could be improved
- the interaction between the private sector provisions and the other provisions of the Act, and between the NPPs and Part IIIA of the Act and
- how the identified issues could be addressed.

¹⁹ Privacy Amendment (Private Sector) Bill 2000 Second Reading Speech 12 April 2000 Representatives Hansard p 15751.
Finally, the issues paper addressed the issue of new developments in technology. This is addressed in Chapter 8.

**Other law impacting on privacy**

**Other provisions of the Privacy Act**

Public and private sector provisions integrated

The private sector provisions were enacted as an amendment to the existing Privacy Act 1988. It was intended that the NPPs would operate alongside the pre-existing provisions of the Act, including the IPPs, which apply to public sector agencies, and the provisions regulating credit reporting (largely contained in Part IIIA of the Act). Although the NPPs are similar to the IPPs, there are differences. Unlike the IPPs, the NPPs include specific provisions about the transfer of data overseas (NPP 9), and the NPPs provide more protection to defined types of ‘sensitive personal information’, including health information. The NPPs and the IPPs are included at Appendices 4 and 5 respectively.

Interaction of private sector provisions with other provisions

There are circumstances when an organisation might be subject to both the NPPs and the IPPs. An Australian Government contractor, for example, may be bound to comply with the NPPs, and will also be bound by contract to comply with the IPPs. Some government enterprises are, for the purposes of the Privacy Act, both an ‘agency’ (in relation to their non-commercial activities) and an ‘organisation’ (in relation to their commercial activities). Similarly, credit providers and credit reporting agencies will generally be an ‘organisation’ for the purposes of the private sector provisions and will be bound by the NPPs as well as the provisions of Part IIIA of the Act which impose specific obligations on them.

**Other Commonwealth legislation**

Overview

A number of pieces of Commonwealth legislation impose obligations on organisations that may have an impact on how those organisations comply with their obligations under the Privacy Act. This legislation is administered by various Australian Government agencies.
Misleading and deceptive conduct

Section 52 of the Trade Practices Act 1974, administered by the Australian Competition and Consumer Commission (ACCC), provides that a corporation shall not, in trade or commerce, engage in conduct that is misleading or deceptive, or is likely to mislead or deceive. This may influence the way in which an organisation complies with NPP obligations such as making people aware it has collected their personal information, openness and giving reasons for denying access or refusing to correct personal information. A similar provision in the Australian Securities and Investments Commission Act 2001 (ASIC Act), administered by the Australian Securities and Investments Commission (ASIC), section 12D, applies to financial services.

Telecommunications

The Telecommunications Act 1997, administered by the Australian Communications Authority (ACA), includes provisions relating to privacy. The Telecommunications (Interception) Act 1979 makes it an offence to intercept communications and specifies the circumstances in which interception may lawfully take place. The Spam Act 2003 establishes a scheme for regulating commercial email and other types of commercial electronic messages. This is discussed in more detail later in this chapter at 2.3.

Other

Other relevant Commonwealth legislation includes the Corporations Act 2001, which limits use or disclosure of information on company shareholder registers (section 177), and the Commonwealth Electoral Act 1918, which regulates access to, and use and disclosure of, electoral roll information. The Australian Broadcasting Authority (ABA) may investigate complaints alleging a breach of broadcasting industry codes, some of which include provisions intended to protect individual privacy, or practice20.

State and territory legislation

New South Wales, Victoria, the Australian Capital Territory and the Northern Territory have privacy legislation that covers all or part of their own public sectors. In Tasmania, similar legislation commences on 1 July 2005. Other jurisdictions have administrative arrangements which seek to establish appropriate information handling practices. Queensland has established two standards for privacy regulation in its public sector on an administrative basis. In South Australia, an administrative instruction applies to government agencies and a Code of Fair Information Practice, based on the NPPs, applies to all personal information handled by the Department of Human Services and its agencies. The Western Australian public sector does not currently have a legislative privacy regime.

---

20 See, for example, the Commercial Television Industry Code of Practice, clause 4.3.5.
Each jurisdiction’s scheme is slightly different and so are the principles on which they are based. In addition, New South Wales and Victoria have health privacy legislation that regulates the handling of personal information in their public sectors and the private sector. They contain similar, though not identical, principles to the NPPs. The Australian Capital Territory has legislation, that predated the NPPs, covering health service providers in the public and private sector. The Australian Health Ministers’ Advisory Council (AHMAC) is currently working towards a National Health Privacy Code, which may be one way of achieving national consistency for the handling of personal health information.

**Other law**

Other obligations overlap with responsibilities imposed on organisations by the Privacy Act. They include:

- legal obligations of confidence (for example, patient/doctor confidentiality and the banker’s duty of confidence) and
- legal professional privilege.

**Self regulatory mechanisms**

A number of industry organisations developed their own codes.

**Telecommunications.** The Australian Communications Industry Forum (ACIF) has developed a number of industry codes and guidelines, some of which deal with matters relating to the handling of personal information.

**Direct Marketing.** The Australian Direct Marketing Association (ADMA) has developed a model code, which includes the NPPs and a reference to the NPP Guidelines. It enforces the code against its members.

**E-marketing.** Following passage of the Spam Act, the Australian eMarketing Code of Practice was registered under Part 6 of the Telecommunications Act.

**Submissions favour national consistency**

Submissions overwhelmingly support the goal of national consistency. Business generally, and the finance and retail industries in particular, think that national consistency is important.

Members of the Australian Finance Conference (63) support the Government’s object of achieving a single comprehensive scheme for handling personal information and it continues to remain important for them. It remains relevant and important to the Australian Bankers’ Association (70). It is ‘essential’ for the financial planning industry says the Financial Planning Association (85). In the view of the Australian Association of Permanent
Building Societies (91), it is ‘imperative’ for there to be a single nationally consistent scheme.

The charity sector agrees. Fundraising Institute Australia Ltd (52) argues that national consistency is important in ensuring compliance and reports that its members advise that consistency would improve their capacity to undertake their work as fundraisers.

Consumers also agree. The Consumers’ Federation of Australia (65), for example, says national consistency is essential for privacy protection for consumers in Australia. The Australian Consumers’ Association (15):

‘endorses the goal of a single, comprehensive, nationally consistent scheme for privacy protection in Australia. Such consistency makes the task of compliance by industry easier and cheaper. It facilitates education.’

On the other hand, in stakeholder forums, consumer groups made the point that they do not want national consistency at the cost of reducing privacy protection to the lowest common denominator.

The health sector, including the private hospital sector, professional organisations and public sector bodies like the Health Services Commissioner, Victoria (27), say there should be nationally consistent health standards. The Royal District Nursing Service (78) says national consistency is ‘vital’.

**Objective has not been achieved**

Despite the almost universal support for consistency, the objective has not been achieved in the view of very many submissions. Business and consumers agree that the objective has not been met. The Australian Consumers’ Association (15), the National Health and Medical Research Council (32), Promina (34), the Consumers’ Federation of Australia (65) and the Australian Health Insurance Association Ltd (76), for example, all agree the objective has not been achieved.

The Australian Chamber of Commerce and Industry (22) says there is a general trend towards ‘fragmentation’, which has ‘adverse consequences in terms of magnified compliance burdens, administrative duplication and overlap between the separate regimes’.

Submissions from business and consumer organisations describe an emergence of a ‘patchwork’ of federal and state and territory legislation, driven by, according to the Consumers Federation of Australia (65):

‘divisions by public and private sectors of the economy, state and federal levels of government, specific economic sectors (such as
health), emerging technologies [and] gaps embodied in the federal legislation'.

Telstra (110) identifies state and territory legislation which contracted service providers must comply with and says that:

‘the proliferation of State-based legislation and inconsistency between State-based and Commonwealth legislation has the potential to add costs to conducting business with Government agencies’.

The Australian Retailers Association (111) describes recently introduced (or about to be introduced) state legislation as ‘designed to subvert the authority of the Federal Privacy Commissioner and create a complicated compliance regime for business.’

ANZ (40) is concerned that Australia will end up with differing laws among states that will confuse customers and increase compliance costs. The Insurance Council of Australia (59) describes privacy law as a ‘patchwork’, as does the Australian Bankers’ Association (70). The Australian Communications Authority (94) says there are gaps, overlap and jurisdictional confusion.

Coles Myer (60), concerned about the introduction of workplace surveillance legislation by the states, says that:

‘as with any other area of regulation (eg tax) any exemptions or possible inconsistencies provide an opportunity for the States and Territories to impose their own requirements’.

What submissions say - issues

State and territory laws are inconsistent with the Privacy Act

Overview

One of the consequences of the lack of national consistency in the way privacy is regulated is that organisations may be subject to inconsistent laws. There are inconsistencies between the Privacy Act and some state and territory legislation. Submissions identify a number of examples of this.

Health services

Health services provided by the private sector are subject to the Privacy Act. They may also be subject to state and territory health records legislation which may not be consistent with the Privacy Act. This is discussed in detail later in this chapter at 2.5.
Welfare organisations

Welfare organisations administer programs that are government funded. They may be funded by both the Australian Government and a state or territory. A charitable organisation (11) points out that in administering its Employment Services and Community Services programs it may have to comply with the NPPs, the IPPs, department procedural requirements and state or territory law. Furthermore, as their Community Services contracts are often negotiated on an individual program basis, the responsibility for interpreting the contractual provisions will fall on local management. The issue is further complicated by the fact that the organisation may need to collect health information as well, which is subject to state or territory health records legislation.

Tenancy databases

The Real Estate Institute of Australia (13) identifies legislation relating to tenancy databases as an example of lack of consistency between federal and state and territory legislation. Its submission to the working group of the Ministerial Council of Consumer Affairs advocated that a nationally consistent framework should be developed for the operation of tenancy databases. In the meantime, Queensland and New South Wales have their own legislation and the Australian Capital Territory is considering it.

Occupational health and safety

St John Ambulance Australia (97) identifies an inconsistency between the Privacy Act and occupational health and safety legislation in the context of reporting casualties at events.

Commonwealth laws are complex

Telecommunications

Submissions have drawn attention to inconsistencies between the Privacy Act and other Commonwealth legislation, for example, between Part 13 of the Telecommunications Act and the Privacy Act in relation to disclosure of customer information. Telecommunications companies may be subject to both. This is discussed in detail later in this chapter at 2.3.

Credit unions

There are other difficulties in the relationship between the Privacy Act and other Commonwealth legislation. The Credit Union Services Corporation (CUSCAL) (64) is concerned that the Corporations Law provides that credit unions must give anyone access to their share register which contains personal information about their shareholders who are also their customers.
Private health insurance

The Private Health Insurance Ombudsman (10) draws attention to difficulties caused by the notion of ‘contributor’ and ‘dependents’ in relation to a private health insurance contract in the National Health Act.

Inconsistency between the NPPs and IPPs

Organisation may be subject to both

There are inconsistencies between the NPPs and the IPPs. Some organisations may be subject to both. Australia Post (109) points out that the IPPs apply to its ‘non-commercial activities’ but the NPPs apply to its commercial activities. In addition, its employees must comply with further, and more specific, obligations of privacy and confidence in the Australian Postal Corporation Act 1989.

Commonwealth contractors

An organisation contracted by the Australian Government (or subcontracted by an Australian Government contractor) to perform outsourced functions for the Australian Government must comply with the IPPs and the NPPs. The contract will require the contractor to comply with the IPPs. Where there is no provision in the contract equivalent to one or more of the NPPs, the NPPs apply.

The Chamber of Commerce and Industry WA (Inc) (77) says that there are aspects of the IPPs which may be problematic or confusing. The Tenants’ Union of Queensland Inc (69), which is funded through the Community Legal Centres funding program, notes that having to comply with both the IPPs and the NPPs is unreasonably cumbersome on community sector organisations.

In the view of Telstra (110), the differences between the IPPs and the NPPs may lead to uncertainty about the obligations that apply when a contracted service provider collects (or otherwise handles) personal information on behalf of an Australian Government agency.

Finally, the Australian Government Department of Health and Ageing (99) identifies inconsistencies that have arisen in the context of Australian Government funded Aboriginal health services. It draws attention to circumstances when compliance with the NPPs alone would, in the appropriate circumstances, allow a doctor to discuss the care of a patient with a relative without the patient’s consent but compliance with the IPPs would not.
An organisation may be subject to several privacy regimes

A number of submissions describe the difficulties they face complying with several privacy regimes at the same time. Promina (34), whose operations are national, is ‘subject to a complex matrix of federal and state legislation’. A confidential submission notes that each business activity is subject to different privacy legislation according to the state or territory the business operates in; the type of business; the type of personal information collected (personal information or health information); and whether the business unit is considered a government agency or a private sector organisation.

The Department of Health and Ageing (99) gives an example of the effect of several layers of privacy regulation. In giving advice to ACT pathologists who were changing their forms in a way that gave rise to privacy implications, the Department had to refer to the Privacy Act (the IPPs and NPPs), the Health Records (Privacy and Access) Act 1997 (ACT) and other ACT legislation, applying to pathologists operating as a private sector organisation.

Single piece of information may be subject to different laws

A number of submissions, particularly those from financial services organisations, have pointed out that one consequence of the plethora of legislation is that a single item of personal information may have several pieces of legislation, possibly inconsistent, applying to it. Promina (34), a group of insurance and financial services companies that operates nationally notes that:

‘a single piece of personal information may be subject to two or more . . . legislative regimes at one time, creating conflicting obligations, different obligations or more onerous obligations in respect of the whole or parts of that same piece of information.’

Suncorp-Metway Ltd (35), another banking, insurance, investment and superannuation conglomerate, notes that the:

‘same piece of personal information may have multiple pieces of legislation applying to it, some of these obligations may compete with others and we may have to quarantine particular parts of that information and apply federal or state laws as applicable.’

There are jurisdictional problems

The plethora of legislation gives rise to jurisdictional problems. This affects both organisations and consumers. Telecommunications companies, for example, are subject to multiple regulators, including, for example, the Privacy Commissioner, the Australian Communications Authority (ACA), and the Telecommunications Industry Ombudsman (TIO). However, Optus (98), which
deals with the ACA, the Office and other government bodies on various aspects of privacy, says that dealing with different regulators has not caused it any difficulties. The ACA (94) says that even the regulator may not know if it has jurisdiction until the investigation has begun.

The Private Health Insurance Ombudsman (10) notes that there is no clear jurisdiction in relation to privacy complaints between the federal and New South Wales Privacy Commissioners. Consequently, a person in New South Wales may complain to both.

ANZ (40) notes that banking customers with a privacy complaint may choose to go to the Banking and Financial Services Ombudsman (BFSO) or to the Privacy Commissioner. In a recent case a customer took part of a complaint to the BFSO and the privacy aspect of it to the Privacy Commissioner. (The whole complaint was ultimately resolved at a conciliation conference between the customer, the bank and the BFSO).

Telecommunications customers may also choose between the TIO and the Privacy Commissioner.

Compliance is more difficult

The lack of a single, national and comprehensive regime increases the administrative and cost burden of compliance on organisations. Submissions from a number of industries have drawn attention to this.

Suncorp-Metway Ltd (35) notes that its staff need to deal with various pieces of legislation and to deal with a number of regulators, ranging from the Privacy Commissioner to the Health Care Complaints Commissions of the states. It notes:

‘this makes the practice of providing information, adhering to the correct legislation and reference to a Regulator difficult for our staff and may result in the incorrect information being provided, incorrect principles or guidelines being applied or information not being fully provided.’

ANZ (40) is particularly concerned that if New South Wales or Victoria introduces their own workplace privacy legislation, which seems likely, the prospect of non-uniform laws throughout Australia would be opened again. Organisations that operate nationally would be subject to contradictory laws affecting the national workforce.

‘This would be likely to create significant additional compliance costs due to systems modifications, altered practices and staff training in order to manage the differences and ensure compliance.’
Comcare (12), which deals with health professionals, says that they are often unsure as to which privacy regime they are subject to when dealing with information relating to people in the Commonwealth jurisdiction.

The Australian Compliance Institute (16) notes that many national health services comply with what they consider to be the more onerous Victorian and New South Wales provisions across all jurisdictions to ensure they need deal with only one compliance system.21

**Difficult to advise**

The Australian Physiotherapy Association (37) notes that inconsistent legislation creates confusion for its members. Furthermore, it creates difficulties for the association itself in keeping abreast of the legislation and putting out a consistent message to its members about their privacy obligations.

**Lack of consistency is getting worse**

Many submissions say that the problem of inconsistency is getting worse. They cite, for example, the proliferation of state and territory health records Acts and the Australian Government’s recently enacted Spam Act. Financial institutions in particular express concern about the developments in workplace surveillance legislation at a state and territory level, and the Real Estate Institute of Australia (13) is concerned that legislation regulating tenancy databases is being introduced in a piecemeal fashion. The Credit Union Services Corporation (CUSCAL) (64) is concerned about proposed anti-money laundering laws that will force credit unions to collect more, not less, personal information about its members. CUSCAL:

> 'is particularly concerned about the need to educate consumers about these obligations and the reasons why privacy rights must yield to security concerns.'

**What submissions say - addressing the issues**

**Australian Government should exercise its constitutional power**

Some submissions suggest that the Australian Government should exercise its constitutional power to ensure that Commonwealth law prevails. A charitable organisation (11) says that the Australian Government should enforce its overriding constitutional power to the extent that all formal complaints about privacy should go to the Privacy Commissioner. The

---

21 There are also consistencies between the Victorian and New South Wales legislation.
Salvation Army Australia Southern Territory (74) argues that Commonwealth law should prevail over state and territory law to provide consistency.

**Review and simplify**

The complex nature of privacy law in Australia leads a charitable organisation (11) to suggest that the legal requirements imposed by privacy law should be reviewed and simplified. The National Health and Medical Research Council (32) says that there should be a single, simplified national health privacy regulatory scheme.

**Greater co-operation among governments**

Submissions from health services raise the lack of consistency between the Privacy Act and state and territory legislation regulating health records as a problem, and a problem that will become worse as electronic medical records become commonplace.

Banks and other financial institutions are concerned that at least two states are developing workplace surveillance legislation independently of each other.

A participant in a stakeholder forum hopes that at least the various bodies might consider a consistent interpretation of terms such as ‘related’ and ‘reasonable’ because currently they are interpreted differently across jurisdictions.

There clearly needs to be greater co-operation between the Australian and state and territory governments in developing legislation that has privacy implications if national consistency is to be achieved. In the view of the Australian Information Industry Association (43), the Australian Government needs to take the lead to ensure that disparate policies do not emerge. The Insurance Council of Australia (ICA) (59) recommends that

‘Federal and State Ministers should work together to ensure that privacy regulation is developed in a coherent and consistent manner. Health ministers should promote co-ordination between the States in the development of privacy legislation.’

Telstra (110) wants to see more co-operation between the Office and other regulators to ensure a national and consistent approach to enforcement.

There needs to be a process for ensuring ongoing Australian and state and territory government co-operation. This has already happened in the area of health privacy. A National Health Privacy Working Group of the Australian Health Ministers’ Advisory Council (AHMAC) is developing a national privacy code. Applauding the commitments of the health ministers, the ICA encourages AHMAC to finalise the health code.
Enhance the Privacy Commissioner’s role

Given the need for a national approach it is appropriate that the Australian Government should take the lead in any process that is established to ensure consistency.

In the view of Telstra (110), the Australian Government should liaise with State and Territory governments to encourage a consistent approach. The Salvation Army Australia Southern Territory (74) urges the Office to take a role in ensuring consistency.

A number of possible mechanisms for doing this are identified in submissions. The Association of Market Research Organisations (AMRO) and the Australian Market and Social Research Society (AMSRS) (61) suggest that there should be a clearing house for ensuring that proposed legislation is consistent with the Privacy Act and that there should be a Privacy Impact Statement made for each new law. In the view of the Australian Bankers’ Association (70), the clearing house should be the Office.

‘The ABA would support the Privacy Commissioner taking a lead role in the oversight and co-ordination of developments in other legislation that have implications for privacy regulation acting as a clearing house to ensure national consistency with the Act wherever possible’.

Other submissions recommend an enhanced role for the Office. The Australian Direct Marketing Association (67) suggests that the Office should be given increased authority to ensure there are appropriate mechanisms to ensure legislation that is inconsistent with the private sector provisions is not passed.

The Australian Nursing Federation (127) suggests that the Office should initiate a process to consult with all stakeholders to develop a single piece of national health privacy legislation.

Coles Myer Ltd (60) suggests the Office should be adequately funded to be involved in proposed laws. In the view of the Credit Union Services Corporation (64), it should also be well enough funded to participate actively in the development of new anti-money laundering laws.

Combine the NPPs and the IPPs

A number of submissions recommend that the NPPs and IPPs be combined into a single set of privacy principles that would apply to both Australian Government agencies and private sector organisations. In the view of a charitable organisation (11), the NPPs should prevail. Electronic Frontiers (51) says that the harmonisation of the two sets of principles should be done so as to provide the highest level of privacy protection from each of them.
Remove exemptions from the Privacy Act

One of the ways to ensure greater national consistency could be to remove the existing exemptions from the Privacy Act. In the view of a number of participants in the stakeholder forums, the exemptions provide gaps in protection that states and territories need to fill with their own legislation. Among the drivers of the development of privacy law in other jurisdictions are the gaps in the protection provided by the federal law. The exemptions in the Privacy Act are undermining the goal of national consistency.

Options for reform

Clarify constitutional issue

The failure of the Privacy Act to achieve its object of establishing a 'single comprehensive national scheme' for the protection of personal information is an issue for the private sector. As submissions reveal, national consistency is important to business, to charities and to individuals. The lack of national consistency contributes significantly to the costs imposed on business. It is not clear whether section 3 of the Privacy Act, which provides that the operation of state and territory laws that are ‘capable of operating concurrently with’ the Act are not to be affected, covers the field or not. This provision determines whether or not a state or territory privacy law, or part of it, is or is not constitutional.

This lack of clarity leaves the way open to a state or territory to pass its own laws on the ground that there is no constitutional barrier to doing so. It certainly may be that state and territory legislation purporting to regulate health records is inconsistent at least to the extent that it imposes obligations on organisations covered by the Privacy Act. If so, it may be unconstitutional. Section 3 could be amended to make it clear that the Privacy Act was intended to cover the field.

Australian Government to promote national consistency

All stakeholders regard national consistency as very important and claim that it has not been achieved. Because of the exemptions in the Privacy Act, some hold the Australian Government at least partly responsible for not achieving the 'single comprehensive national' scheme it promoted. It is also a consequence of our federal system. It is clearly the role of the Australian Government, rather than the states and territories, to play the leadership role in promoting national consistency. To succeed it has to be done at the highest level. The Australian Government could ask the Council of Australian Governments (COAG) to endorse national consistency in all privacy related legislation.
Consult Privacy Commissioner about all privacy related legislation

There would be more consistency in privacy related legislation if a centralised body had oversight of all proposed legislation. One possibility is that the Privacy Commissioner plays that role. The Privacy Commissioner is already consulted when Australian Government policy affecting privacy is being developed. Even if desirable, it may not be practical to nominate a federal body to play such a role in relation to the states and territories.

Examine IPPs and NPPs

The lack of consistency between the IPPs and the NPPs causes considerable compliance difficulties for organisations that are public sector organisations that undertake commercial activities and for some private sector organisations, especially those who are funded by Australian Government agencies or are contracted to Australian Government agencies. Although both sets of principles draw on the 1980 Organisation for Economic Co-operation and Development (OECD) Guidelines for the Protection of Privacy and Transborder Flows of Personal Data, each set of principles reflects the time in which it was developed.

Similar functions are performed by both public and private sector bodies, and both public sector and private sector bodies may be characterised as both an agency and an organisation for the purposes of the Privacy Act. There seems no clear rationale for applying similar, but slightly different, privacy principles to public sector agencies and private sector organisations and certainly no clear rationale for applying both to an organisation at the same time. There is no clear policy reason why they are not consistent. The time may have come for a systematic examination of both the IPPs and the NPPs with a view to developing a single set of principles that would apply to both Australian Government agencies and private sector organisations.

Consider Australian Government contractors

As part of the suggested examination of the IPPs and NPPs the application of both the IPPs and the NPPs to Australian Government contractors could be considered.

Power to make a binding code

When state and territory governments pass legislation regulating activities that businesses engage in on a national basis that is not uniform, there is a negative impact on business.
Having to comply with similar but different legislation in the states and territories adds to the costs and complexity of compliance.

One way of overcoming the problems caused by inconsistent state and territory legislation regulating a particular activity is to provide for a power within the Privacy Act to develop binding codes. There are a number of ways in which this could be achieved. For example, the Attorney-General, after identifying the need for a code in a specific sector, could ask the Privacy Commissioner to commence a process to develop a code in consultation with key stakeholders. The Privacy Act would need to be amended to provide a power for the Privacy Commissioner to develop a code following a request from the Attorney-General.

A model that is worth considering is that set out in the Trade Practices Act 1974. The Act provides by regulation for the Minister to declare a code mandatory for the industry in question.

Alternatively, the Privacy Act could be amended to provide for the Privacy Commissioner, at his or her own initiative, to make a binding code in appropriate circumstances, again drawing on strong stakeholder consultation.

A model that may be worth considering is that set out in the Telecommunications Act. The Act provides for the telecommunications industry to develop self regulatory codes on a range of matters including privacy. Section 125 of the Act provides a mechanism for the regulator, the Australian Communications Authority, to issue a binding industry standard where a self regulatory code is failing or where no code has been developed. The process places strong emphasis on stakeholder consultation.

**Change the name of the Office to the Australian Privacy Commission**

Section 19 of the Privacy Act established the Office of the Privacy Commissioner, also known as the Office of the Federal Privacy Commissioner. The NSW Office is known as the Office of the NSW Privacy Commissioner or Privacy NSW; the Victorian Office is the Office of the Victorian Privacy Commissioner or Privacy Victoria.

The similarity of these names causes confusion, especially for consumers who are trying to work out to whom they should make a complaint. Changing the name of the Office would avoid unnecessary confusion. It would also be more consistent with other Australian Government regulatory bodies, such as the Australian Competition and Consumer Commission and the Australian Securities and Investments Commission.
2.2 Recommendations: National consistency

The Privacy Act has not achieved its object of establishing a ‘single comprehensive national scheme’ for the protection of personal information. As submissions reveal, national consistency is important to business, to charities and to individuals. The lack of national consistency contributes significantly to the costs imposed on business.

2 The Australian Government should consider amending section 3 of the Privacy Act to remove any ambiguity as to the regulatory intent of the private sector provisions.

3 The Australian Government should consider asking the Council of Australian Governments (COAG) to endorse national consistency in all privacy related legislation.

4 The Australian Government should consider setting in place mechanisms to address inconsistencies that have come about, or will come about, as a result of exemptions in the Privacy Act, for example, in the area of workplace surveillance.

5 The Australian Government should consider commissioning a systematic examination of both the IPPs and the NPPs with a view to developing a single set of principles that would apply to both Australian Government agencies and private sector organisations. This would address the issues surrounding Australian Government contractors.

6 The Australian Government should consider changing, by legislative amendment, the name of the Office of the Privacy Commissioner to the Australian Privacy Commission.

7 The Australian Government should consider amending the Privacy Act to provide for a power to make binding codes.
2.3 Consistency in telecommunications

Law and policy

Businesses in the telecommunications sector handle a large range of personal information, including customer details, telephone or internet service details, as well as carrying the contents of telecommunications such as voice calls, SMS and MMS messages, and emails.

Telecommunications carriers, as a group, collect personal information about all telephone and internet subscribers, amounting to a very large proportion of the population. There are 11.7 million fixed telephone lines in Australia, 16.5 million mobile phone services, and 5.2 million internet subscribers. Some of this information is routinely transferred between telecommunications carriers as an integral part of the operation of the telecommunications network. Telecommunications carriers also hold information of interest to emergency services and law enforcement agencies.

In addition to information about subscription to telephone, internet and other telecommunications services (e.g. name, address, phone number etc.), the contents of voicemails, emails, SMS and MMS messages can include some of the most sensitive and personal information we have. Such messages are often stored, for varying lengths of time, by telecommunications companies.

The community’s interest in protecting the privacy of telephone calls and other telecommunications is reflected in a range of legislation that pre-dates the private sector provisions of the Privacy Act. The Office’s community attitude research shows that individuals are more reluctant to give organisations their home phone number than all other sorts of information, with the exception of bank account details and income. The Office’s research also shows that this sensitivity has increased over recent years.

The private sector provisions of the Privacy Act regulate organisations that operate within the telecommunications sector. These provisions do not, however, include specific references to the telecommunications sector. Telecommunications-related businesses with a turnover less than $3 million may not be covered by the Privacy Act.

In the telecommunications sector, privacy is also regulated through the Telecommunications Act 1997 (Telecommunications Act), the Telecommunications (Interception) Act 1979 (Interception Act), and the Spam Act 2003 (Spam Act).

A number of submissions focused on the regulation of telecommunications privacy in considering the question of national consistency. Many of these

---

22 Figures for 30 June 2004, reported in the Australian Communications Authority Telecommunications Performance Report 2003-04.
submissions referred in particular to the operation of the Privacy Act with the Telecommunications Act, in some cases analysing in detail the interaction of specific provisions of both Acts.

Telecommunications Act

Part 13 of the Telecommunications Act provides for the confidentiality of personal information and the contents of communications, including restrictions on how telecommunications carriers and carriage service providers may use and disclose information that relates to the affairs of other persons, the contents of communications, and the services they provide. The Privacy Commissioner has the function of monitoring compliance with the record-keeping requirements in Division 5 of Part 13 of the Telecommunications Act.

Part 6 of the Telecommunications Act provides for industry to develop binding codes, for example codes developed by the Australian Communications Industry Forum, which are registered with the Australian Communications Authority. The private sector provisions of the Privacy Amendment (Private Sector) Act 2000 include amendments to Part 6 of the Telecommunications Act, and were intended to recognise and promote the pre-eminence of the Privacy Act and the role of the Privacy Commissioner within the telecommunications environment without diminishing the integrity of the telecommunications self-regulatory regime.

Industry codes provide a mechanism that permits the inclusion of privacy provisions beyond those in the Privacy Act, where the telecommunications industry considers that the NPPs do not readily address some specific industry or service related privacy concern. The Privacy Commissioner has a statutory role during the development phase of industry codes that relate to privacy, which involves the telecommunications sector consulting the Privacy Commissioner about such codes.

Telecommunications (Interception) Act

The Telecommunications (Interception) Act 1979 (Interception Act) has two key purposes. Its primary object is to protect the privacy of individuals who use the Australian telecommunications system by making it an offence to intercept communications. The second purpose of the Interception Act is to specify the circumstances in which it is lawful for interception to take place.

Following amendments to the Interception Act in 2004, stored communications such as emails, SMS and MMS messages are not protected by the prohibition on interception and the associated penalties in the Interception Act. Submissions made no substantial comment on the Interception Act or its interaction with the Privacy Act.
Spam Act

The Spam Act 2003 (Spam Act) sets up a scheme for regulating commercial email and other types of commercial electronic messages. Under the Spam Act, unsolicited commercial electronic messages must not be sent, and there are restrictions on the use of address-harvesting software.

Telecommunications regulators

There is more than one regulator with an interest in privacy in the telecommunications sector. The Australian Communications Authority (ACA) monitors the performance of telecommunications carriers and carriage service providers. The Telecommunications Industry Ombudsman (TIO), set up by the industry, investigates complaints about a range of telecommunications issues, including printed and electronic White Pages, privacy and breaches of the Customer Service Guarantee, and industry Codes of Practice.

Complaints and enquiries

During the review reporting period (21 December 2001-31 January 2005), approximately 9% of all NPP complaints received by the Office (223 complaints) related to the telecommunications sector, positioning it as the third most complained about sector behind the finance and health sectors. The Office also received 1725 telecommunications enquiries over the period, or approximately 4% of NPP enquiries.

The Telecommunications Industry Ombudsman, which also deals with some privacy-related complaints in the telecommunications sector, reports that in the 2003-2004 year, it dealt with 1271 telecommunications complaints that related directly to issues concerning privacy. This suggests that the Office’s NPP complaints represent approximately 6% of the privacy complaints in the telecommunications industry.24

Compared to all NPP complaints received in the reporting period, complaints against telecommunications sector organisations were much more likely to concern use and disclosure issues and much less likely to concern access issues.25

---

24 The TIO deals with complaints relating to credit matters in the telecommunications industry, and it may be that some of the 1271 privacy-related complaints it dealt with in 2003-2004 involved credit privacy issues. The Office also deals with complaints relating to the credit reporting provisions of the Privacy Act under Part IIIA, however the number of these complaints are not reflected in the figures in the text.

25 For example, over half of the NPP complaints received against telecommunications sector organisations concerned use and disclosure issues under NPP 2, compared to approximately one third of all NPP complaints.
The following graph shows the NPP complaints received by the Office against telecommunications sector organisations according to the issues raised in the complaint.26

<table>
<thead>
<tr>
<th>Issue Type</th>
<th>Complaints Received from 21 Dec 01 - 31 Jan 05</th>
</tr>
</thead>
<tbody>
<tr>
<td>Collection Use and Disclosure</td>
<td>51</td>
</tr>
<tr>
<td>Data security issues</td>
<td>42</td>
</tr>
<tr>
<td>Data quality issues</td>
<td>36</td>
</tr>
<tr>
<td>Refused access</td>
<td>19</td>
</tr>
<tr>
<td>Other</td>
<td>5</td>
</tr>
</tbody>
</table>

Disclosure of silent numbers

The disclosure of silent numbers by telecommunications carriers was possibly the most recurrent single issue in NPP complaints received against telecommunications sector organisations. Similarly, the disclosure of silent numbers was a recurrent issue in the ten own motion investigations into organisations in the telecommunications sector commenced by the Privacy Commissioner under section 40(2) in the Act, during the reporting period. These figures reinforce the results in the Office’s community attitude survey about the sensitivity of telephone numbers in the community.

Some of the own motion investigations in the telecommunications sector related to the personal information of many hundreds, and even thousands, of individuals.

Complaints closed

A total of 181 NPP complaints against telecommunications sector organisations were closed in this period of which 34 were closed as adequately dealt with under section 41(2)(a) of the Privacy Act following investigation or preliminary enquiries by the Office. An analysis of the number of complaints closed under this provision provides an indication of the number of complaints that were substantiated by the Office.

26 A similar graph showing all NPP complaints received by issue type is included in the Compliance section of this report. It should be noted that complaints may be recorded under more than one issue type, and so the total number of complaints by issue type may exceed the total number of complaints.
The following graph indicates the issues raised in NPP complaints against telecommunications sector organisations that were closed under section 41(2)(a)\textsuperscript{27}. As with complaints received against this sector, over half of the 34 complaints closed under this provision concerned use and disclosure issues.

![Complaints Resolved by Respondent following intervention by OPC](chart)

<table>
<thead>
<tr>
<th>Issue Type</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>Collection</td>
<td>2</td>
</tr>
<tr>
<td>Disclosure</td>
<td>18</td>
</tr>
<tr>
<td>Data quality issues</td>
<td>11</td>
</tr>
<tr>
<td>Data security issues</td>
<td>8</td>
</tr>
<tr>
<td>Refused access</td>
<td>3</td>
</tr>
</tbody>
</table>

The operation of other laws

Some use and disclosure complaints against telecommunications sector organisations may have been closed where it was assessed that the use or disclosure was required or authorised by or under another law. In addition, seven of the 181 NPP complaints against telecommunications organisations closed in the reporting period were declined, having been assessed as being more appropriately or currently dealt with under another law, including the Telecommunications Act.

Small business exemption

The Office recently contacted a wide range of Internet Service Providers (ISPs) in the course of its enquiries into an industry-wide practice. At least 25% of the ISPs that responded advised that they could claim the small business exemption. Between 10 and 15% of telecommunications sector respondents to NPP complaints received by the Office were ISPs.

What the submissions say - issues

Overlap of privacy and telecommunications legislation

Electronic Frontiers Australia (51) argues that the telecommunications sector has, of necessity, access to a great deal more information about individuals than do most private sector organisations. This information not only relates to

\textsuperscript{27} As with the previous graph, complaints may be recorded under more than one issue type.
customers, but also to the public in general, and includes the contents of their communications.

To illustrate the scope and importance of the personal information at issue in this sector, Electronic Frontiers Australia (51) quotes at length from an internet service provider executive who said, in 2000 that:

‘we have the username and password for every one of our users, we have their credit card details, we have a lot of information about their liquidity, we can know about every purchase they make online, with whom, when and for how much. We can know every site they visit on the web – every page, every newsgroup, every picture they look at. We could read all of their e-mail and know all about their romances and the jobs they’re applying for. The commercial opportunities arising from this are endless …’.

Telstra (110) says that there is an over-regulation of privacy and information-handling practices, causing regulatory uncertainty and additional compliance costs. Telstra also submits, however, that the private sector provisions of the Privacy Act are working well, and that industry-specific regulation such as Part 13 of the Telecommunications Act is working well.

Electronic Frontiers Australia (51) expresses concern that, in the online environment, individuals have almost no privacy rights, and the obligations that do exist may be difficult to have enforced. It argues that this arises from factors such as uncertainty regarding the definition of ‘personal information’, the ability of organisations to collect personal information without an individual’s consent, the use of ‘bundled’ consents, the small business exemption and technological developments.

Protections on use and disclosure

Sensis (84), the Australian Communications Authority (94), and Electronic Frontiers Australia (51) note that Part 13 of the Telecommunications Act contains different standards for the use and disclosure of personal information than does NPP 2.

Uses and disclosures permitted by the Telecommunications Act

Section 303B of the Telecommunications Act provides that uses and disclosures of personal information that are permitted by Divisions 3 and 4 of Part 13 of that Act, are ‘authorised by law’ for the purposes of the Privacy Act. The Telecommunications Act also allows legal proceedings or administrative action to be taken under both the Telecommunications Act and the Privacy Act, in relation to uses and disclosures of personal information.28

Telstra (110) suggests that despite the provisions of section 303B of the Telecommunications Act, there may still be uncertainty regarding whether a

---

28 See section 303C of the Telecommunications Act.
disclosure of customer information that falls within one of the exceptions in Division 3 or 4 of Part 13 of the Telecommunications Act may nonetheless breach the NPPs or the credit reporting provisions in Part IIIA of the Privacy Act.

Uses and disclosures permitted by NPP 2

Electronic Frontiers Australia (51) raises a further question about the interaction between the Privacy Act and the Telecommunications Act in that section 280(1)(b) of the Telecommunications Act provides that uses and disclosures that are required or authorised by another law are not prohibited by Part 13 of the Telecommunications Act. One possible interpretation of this provision is that the uses and disclosures permitted by the secondary purpose exceptions to NPP 2.1 (for example, for direct marketing) may be available to telecommunications companies, in addition to the exceptions in Part 13 of the Telecommunications Act.

Different standards of protection

Section 289 of the Telecommunications Act permits the use or disclosure of personal information if the person to whom the information relates is either reasonably likely to be aware of the use or disclosure, or has consented to it. Electronic Frontiers Australia (51) argues that section 289 of the Telecommunications Act offers greater privacy protection in relation to use or disclosure for the primary purpose of collection than does NPP 2. For secondary purposes, however, that section is significantly less protective. Unlike NPP 2, section 289 of the Telecommunications Act does not require the use or disclosure to be related to the purpose of collection. As a consequence, a disclosure for a secondary purpose may be permitted by section 289, but not by NPP 2.

Electronic Frontiers Australia (51) also argues that section 291 of the Telecommunications Act is less privacy protective than NPP 2, for example, allowing disclosures for the unrelated secondary purpose of direct marketing by other organisations. Electronic Frontiers Australia also identified section 290 as requiring attention in relation to the disclosure of personal information about third parties.

Section 285 of the Telecommunications Act relates to the use and disclosure of customer information to produce public number directories, and includes a prohibition on the use or disclosure of customer information in connection with a directory with a reverse search capability (that is, where searching on a number provides a person’s name and address). Sensis (84) suggests that the NPPs, rather than industry specific regulation, would be adequate regulation in relation to reverse search functionality.
Small business exemption

A number of submissions noted that the small business exemption may leave unregulated some organisations operating in, or close to, the telecommunications sector.

The Australian Communications Authority (94) notes that Part 13 of the Telecommunications Act does not apply to producers of public number directories (including list brokers). Where a public number directory producer falls within the small business exemption of the Privacy Act, then there may be few or no privacy protections in place.

Electronic Frontiers Australia noted that a range of smaller businesses could fall under the small business exemption, including internet service providers (ISPs), resellers of carrier and/or ISP services; carriage service intermediaries and telecommunications contractors. This is confirmed by the Office’s experience, which suggests that approximately 25% of ISPs may claim the small business exemption.

After the private sector provisions of the Privacy Act commenced in December 2001, the Australian Communications Authority decided to de-register the code ACIF 523 - Protection of personal information of customers of telecommunications providers (October 2001) (CPI Code), to avoid a duplication in the telecommunications privacy jurisdiction 29.

The CPI Code applied to large telecommunications companies, as well as small businesses including ISPs, resellers of carrier and/or ISP services, carriage service intermediaries and telecommunications contractors.

Electronic Frontiers Association (51) says that a net result of the introduction of the private sector provisions and the removal of the CPI Code may be that individuals currently have less protection, overall, in relation to the handling of their personal information by small businesses in the telecommunications sector, than they did prior to 2001. Given the nature and scope of the personal information that is collected, used and disclosed by the telecommunications sector, there would appear to be a notable gap in privacy regulation.

These considerations are also relevant to the broader consideration of the small business exemption in Chapter 6.

Telecommunication regulators

Submissions generally do not indicate that regulatory overlap is a major problem in the telecommunications sector, however there are issues...

---

29 It was felt that there was very little difference between the NPPs and the CPI Code and that, essentially, the requirements in the CPI Code mirror those in the NPPs. If the CPI Code was not de-registered, the telecommunications sector would have been subject to two essentially identical privacy regimes under the NPPs and the CPI Code, enforceable by the Privacy Commissioner and the Australian Communications Authority respectively.
deserving attention according to the Australian Communications Authority (94), Optus (98), and Telstra (110). For example, the Australian Communications Authority says that in the handling of complaints, while regulatory overlap may not have been a significant barrier to resolving complaints, it may have led to some delays, frustration and waste (94).

Spam

Submissions highlighted the recent Spam Act as an example of appropriately specific legislation to deal with a particular challenge posed by new technology.

**What submissions say - addressing the issues**

**Overlap of privacy and telecommunications legislation**

No change required

Telecommunications companies Virgin Mobile (26), Optus (98), Telstra (110) and Vodafone (112) are generally opposed to further regulation, however some call for further clarification of specific issues (see below). Virgin Mobile (26) considers the current level of regulation applying to telecommunications companies to be very significant and that further regulation is not warranted, noting that the current set of legislative requirements impose significant compliance costs.

**Protections on use and disclosure**

**Uses and disclosures permitted by the Telecommunications Act**

Telstra submitted that Part 13 of the Telecommunications Act should be amended to clarify that a disclosure that fits an exception to Part 13 of the Telecommunications Act is not a breach the Privacy Act, or that the Office should publish information sheet outlining its views in relation to privacy complaints in the telecommunications sector.

**Uses and disclosures permitted by NPP 2**

Electronic Frontiers Australia (51) recommends that the law be clarified to ensure that NPP 2.1 does not authorise uses or disclosures that would otherwise be in breach of the Telecommunications Act.

**Different standards of protection**

A range of submissions from consumer and industry perspectives feel that the relationship between the Telecommunications Act and the Privacy Act could be further clarified, either through additional guidance or through legislative
Electronic Frontiers Australia (51) argues that privacy protections should be at least maintained, and in some cases strengthened, in the course of that clarification.

Optus (98), Telstra (110) and Electronic Frontiers Australia (51) saw merit in considering the appropriateness of the privacy protections in Part 13 of the Telecommunications Act. Optus argues that, notwithstanding the usefulness of Part 13 of the Telecommunications Act, it would be beneficial to review it with the aim of making it easier to interpret.

**Small business exemption**

Electronic Frontiers Australia (51) recommends that the small business exemption be deleted from the Privacy Act.

**Telecommunications regulators**

Telstra (110) suggests that in the first instance complaints should be investigated by the appropriate industry body, for example the TIO.

**Spam**

A range of submissions suggest that the relationship between the Spam Act and the Privacy Act could be further clarified, for example through guidance issued jointly by the Office and the Australian Communications Authority. In particular, the different approach to ‘opting out’ between NPP 2.1(c) and the Spam Act was noted by both industry (for example the Australian Bankers Association 70) and consumers (for example, Electronic Frontiers Australia 51). For more discussion on direct marketing see Chapter 4.

**Options for reform**

Overall it appears from the submissions that the combination of general privacy regulation through the Privacy Act, with technology and sector-specific regulation, is working reasonably well in many areas relating to the telecommunications sector.

**Overlap of Privacy and Telecommunications legislation**

Exclude telecommunications from the Privacy Act

While excluding telecommunications companies from the Privacy Act may simplify the regulatory arrangements for companies that operate solely in the telecommunications sector, the additional protections offered by NPPs, particularly relating to collection, data quality, data security and access, would

---

30 For example, Electronic Frontiers Australia, 51, Sensis, 84, and Telstra, 110.
31 Electronic Frontiers Australia (51), Australian Bankers Association (70), Australian Communications Authority (94), and Telstra (110).
be foregone. There does not appear to be sufficient reason to support this option, particularly considering the special nature and broad scope of personal information handled in the telecommunications sector.

As telecommunications is the third most complained about sector under the NPPs, it appears that the Privacy Act provides an important contribution to protecting privacy in this sector.

Repeal Part 13 of the Telecommunications Act

While repealing Part 13 of the Telecommunications Act may simplify the regulatory arrangements for companies that operate in the telecommunications sector, the relatively strong protections on use and disclosure of telecommunications-related personal information offered by Part 13 of the Telecommunications Act would be foregone. There does not appear to be sufficient reason to support this option, particularly considering the special nature and broad scope of personal information handled in the telecommunications sector.

The relatively large number of privacy-related complaints handled by the Telecommunications Industry Ombudsman may suggest that the regulatory scheme provided by the Telecommunications Act is critically important to protecting privacy in this sector.

Transfer Part 13 of the Telecommunications Act to the Privacy Act

The intention of this option would be to retain the protections of both the NPPs and Part 13 of the Telecommunications Act, but to do so under the one Act. In doing so, careful consideration would have to be given to the relationship between the definition of ‘personal information’ in the Privacy Act, and ‘information’ as used in Part 13 of the Telecommunications Act. Similarly, careful consideration would have to be given to whether the requirement in section 16B of the Privacy Act that the Privacy Act applies only to the collection of personal information for inclusion in a record (or a generally available publication) would narrow the application of the provisions of Part 13 of the Telecommunications Act, were they to be transferred to the Privacy Act.

Guidance

Detailed guidance, issued jointly by the Office and the ACA may assist in increasing understanding of the interaction of the Privacy and the Telecommunications Act. This guidance could concentrate on the issues raised in the submissions, such as the operation of section 303B of the Telecommunications Act. Detailed guidance could also assist to clarify that the exceptions to NPP 2 do not provide an ‘authorisation’ under law, for the purposes of other Acts such as the Telecommunications Act.

However, where there is genuine legal uncertainty about the joint operation of the two acts, guidance would not assist.
Amendments to the Privacy Act and the Telecommunications Act

Changes to the Privacy Act alone are unlikely to resolve concerns about the potential for inadequate or inconsistent use and disclosure protections. The overall standard of protection for personal information, set by the combination of Part 13 of the Telecommunications Act and the Privacy Act, could be addressed through coordinated amendments to those Acts which clarify their relationship, particularly in terms of the respective provisions concerning what constitutes authorised uses and disclosures under the two Acts.

At a minimum, amendments could clearly specify that the Privacy Act cannot be used to lower the overall standard of privacy protection, so that an exception under NPP 2.1 cannot ‘authorise’ a use or disclosure under section 280(1)(b) of the Telecommunications Act. For example, it should be clear that a disclosure permitted by NPP 2.1(c), for a secondary purpose of direct marketing, would not, through appealing to NPP 2.1(c), also be permitted by section 280(1)(b) of the Telecommunications Act. Amendments should clarify that if a use or disclosure of personal information is not permitted by Part 13 of the Telecommunications Act considered in the absence of the Privacy Act, then it is not permitted even when considered in the context of the Privacy Act.

Amendments to ensure that the higher privacy standard always operates

Recognising the significant quantity, scope and sensitivity of the personal information that is held by, and that flows through, organisations in the telecommunications sector, a further step could be to amend both the Privacy Act and the Telecommunications Act to ensure that the higher privacy standard always operates. This would require amending or repealing section 303B of the Telecommunications Act to ensure that uses or disclosures prohibited by NPPs 2, 7 and 9 are not permitted by the Telecommunications Act, unless there is a clear, sector-specific requirement that meets the public policy goals of the private sector privacy regulatory scheme.

Small Business Exemption

Public number directory producers are authorised under the Telecommunications Act to access the Integrated Public Number Database (IPND). The IPND is a database of all listed and unlisted telephone numbers. It is a repository of personal information (including names and addresses) relating to the end-users of telephone numbers. According to the Australian Communications Authority:

> ‘In addition to the publication of public number directories, Public Number Directory Producers (PNDPs) are understood to use telecommunications customer information for a variety of other purposes. These uses are referred to by the industry as ‘database
enhancement’, ‘data cleansing’, ‘data verification’, ‘list management’ services or ‘information management tools’.

Some of the significance of IPND data is that it provides a means for directly contacting a large proportion of the Australian population. The use of telephone numbers to direct market is discussed in Direct Marketing, Chapter 4, including evidence from submissions both that there is a level of irritation in the community about the intrusiveness of phone marketing, and that some customers like direct marketing. The option of establishing a ‘Do Not Contact’ register is also discussed there.

The Australian Communications Authority has decided to determine an industry standard to regulate the use of telecommunications customer information. The Office understands that this standard, in conjunction with the NPPs, will aim to regulate the appropriate use of IPND data.

Producers of public number directories clearly handle personal information, and typically in quantity. In the case of any public number directory producer that has an annual turnover of less than $3 million, there may then be some uncertainty about whether or not the small business exemption applies.

Subsections 6D(4)(c) and (d) provide that a business is not eligible for the small business exemption if it trades in personal information. Subsections 6D(7) and (8), however, permit a business that has an annual turnover of less than $3 million, and trades in personal information, to nonetheless benefit from the small business exemption if the trading in personal information is conducted with the consent of the individuals whose information is traded, or if another law requires or authorises the trading of the information.

Regulate-in small telecommunications businesses

The small business exemption could be removed for a nominated class of telecommunications-related small businesses and public number directory producers, by way of a regulation under section 6E of the Privacy Act. This option is less likely to lead to the kind of regulatory confusion that may arise under other options (outlined below). However, it has the disadvantage of further complicating the nature of the small business exemption.

Telecommunications businesses not eligible for the small business exemption

An alternative to regulation would be to amend the Privacy Act to provide that telecommunications businesses and public number directory producers are not eligible for the small business exemption. This may have the disadvantage of further complicating the structure of the small business exemption.

Self-regulatory privacy code registered with the ACA

Making use of the self-regulatory scheme for the telecommunications sector, under the Telecommunications Act, a new telecommunications industry privacy code could be registered with the Australian Communications Authority, so that all telecommunications organisations and public number directory producers will have NPP obligations through that means.

Disadvantages with this approach include the duplication of privacy regulation for the great majority of telecommunications companies who are already bound by the Privacy Act, and are also bound by registered industry codes, and the confusion and uncertainty that may arise as a result; and a further splintering of privacy regulation, because the Privacy Commissioner may not be the complaint handler for all privacy complaints in the sector.

Commissioner to issue mandatory code

If the Commissioner had a power to issue a mandatory code which covered a certain group of businesses (see recommendation 7), this power could be used to develop and issue a telecommunications sector privacy code.

Remove the consent provisions from the small business exception

This would ensure that all organisations that ‘trade’ in personal information (as described by subsections 6D(4)(c) and (d) of the Privacy Act) would be regulated by the Privacy Act. This would assist in ensuring that public number directory producers cannot make use of the small business operator exemption. This option is also discussed in Chapter 6, Small Business Exemption.

Overlapping regulators

See Chapter 5, Complaint Handling, for further discussion of options for minimising problems arising from overlapping regulators.

Spam

The issue of different standards for opting out of direct marketing is taken up in Chapter 4, Direct Marketing. Beyond the recommendations there, the Office and the Australian Communications Authority could work together to issue joint guidance on the operation of the Privacy Act and the Spam Act.
2.4 **Recommendations:**

**Telecommunications consistency**

<table>
<thead>
<tr>
<th>No.</th>
<th>Recommendation</th>
</tr>
</thead>
<tbody>
<tr>
<td>8</td>
<td>The Australian Government should consider amending the Privacy Act and the Telecommunications Act to clarify what constitutes authorised uses and disclosures under the two Acts, and to ensure that the Privacy Act cannot be used to lower the standard of privacy protection in the Telecommunications Act.</td>
</tr>
<tr>
<td>9</td>
<td>The Australian Government should consider making regulations under section 6E of the Privacy Act to ensure that the Privacy Act applies to all small businesses in the telecommunications sector, including Internet Service Providers and Public Number Directory Producers.</td>
</tr>
<tr>
<td>10</td>
<td>The Office will discuss with the Australian Communications Authority the development of guidance to clarify the relationship between the private sector provisions of the Privacy Act and Part 13 of the Telecommunications Act.</td>
</tr>
<tr>
<td>11</td>
<td>The Office will discuss with the Australian Communications Authority the development of guidance to clarify the relationship between the private sector provisions of the Privacy Act and the Spam Act.</td>
</tr>
</tbody>
</table>
2.5 Consistency in protection of health information

Research on community attitudes towards privacy, conducted by the Office, shows the importance that Australians place on the protection of their health information. There are risks of serious harm arising from a failure to adequately protect an individual’s health information, for example when handling genetic information that indicates an individual’s susceptibility to a serious disease or information about an individual’s sexual health. Some individuals may be stigmatised or discriminated against if their health information is mishandled.

While a health service provider’s principal concern is for the health care of their patient, the individual’s right to have their health information protected, and to retain control over it, is also important.

Law and policy

Privacy regulation for health information across Australia consists of a set of overlapping, incomplete and sometimes inconsistent federal, state and territory legislation. The shared intent is to regulate the handling of this sensitive information, and to ensure its protection. However, the multiplicity of laws and provisions, many very similar but not the same, results in confusion and undue complexity.

Commonwealth, state and territory privacy legislation

At the Commonwealth level, the handling of health information is regulated in the private sector and Australian Government public sector through the Privacy Act by the National Privacy Principles (NPPs), the Information Privacy Principles (IPPs) and Public Interests Determinations.

Some state and territory jurisdictions have developed privacy legislation for their public sectors. Others have administrative arrangements for this purpose. For example, Queensland has established two administrative standards for privacy in its public sector (one scheme for health sector agencies, and one scheme for other government agencies). Each

---

33 2004 Research into Community attitudes towards Privacy in Australia (released 26/10/04); 2001 Research into Community, Business and Government attitudes towards Privacy in Australia (released 31/7/01)
jurisdiction’s scheme is slightly different, as are the principles on which they are based.

For privacy in the private sector, two states (in addition to the ACT, which in 2001 already had law covering health services in the private sector) have enacted law seeking to regulate the handling of health information in the private sector. Victoria has enacted the Health Records Act 2001 and in NSW, the Health Records Information Privacy Act 2002 came into force on 1 September 2004.\(^{37}\) These Acts contain similar, though not identical, principles to the NPPs. For example, the Victorian legislation has certain provisions regarding access to ‘old’ personal health information; there are no equivalent provisions in the NPPs.\(^ {38}\)

Other forms of regulation

Additionally, there are other forms of protection for an individual’s health information. These include ethical and professional codes of conduct adhered to by health professionals, common law obligations of confidence that health professionals must abide by, as well as federal, state and territory statutes about matters such as public health. Also, the enabling legislation of many health agencies often contains secrecy provisions.

Proposed National Health Privacy Code

At the request of Health Ministers, the National Health Privacy Working Group of the Australian Health Ministers’ Advisory Council was set up in 2000 to develop a national framework for health privacy. This proposed framework has become known as the National Health Privacy Code.

After public consultation on the draft code in 2003, a revised version, as well as draft mandatory guidelines for research, and draft explanatory notes for the use or disclosure of genetic information, were developed.\(^ {39}\) These documents are yet to be considered by Health Ministers. The Department of Health & Ageing (99) states this will occur in 2005.

**What the submissions say - issues**

Problems for health privacy

Submissions overwhelmingly support the conclusion that the existing state of health privacy laws in Australia is unsatisfactory for health service providers and individuals.


Submissions from health services (and organisations representing them) and from insurers identify problems raised by this lack of consistency. A confidential submission says that health insurers, for example, have gone to the expense of setting up systems consistent with the private sector provisions and then have had to look at separate state and territory legislation, regulations and guidelines, involving them in more expense. The Investment and Financial Services Association Ltd (89) says that the inconsistencies cause a significant compliance burden, resulting in increased compliance costs for many of their member organisations. Furthermore, inconsistencies make it difficult for consumers to understand their rights.

The experience of the Office also indicates that this issue represents one of the biggest obstacles to effective and consistent national developments in the health sector, such as electronic health records systems.

The Australian Law Reform Commission (ALRC) and Australian Health Ethics Committee (AHEC) considered the need for harmonisation of privacy regulation in the context of protecting genetic information. Their report recommended ‘as a matter of high priority’, the development of nationally consistent rules for the handling of all health information40. This has also been acknowledged in regard to other national initiatives, such as HealthConnect41.

Obstacles to national consistency

The obstacles to national consistency in health privacy protection are summarised by the Insurance Council of Australia (59):

- Inconsistencies between state and territory legislation and the Privacy Act (federal)
- Additional obligations imposed by state and territory legislation, over and above the Privacy Act
- Differences between the various state and territory regimes.

Submissions identify a number of recurring issues which are discussed below.

Compliance issues

A number of submissions noted the additional compliance costs which are incurred by having multiple layers of privacy legislation.

---

40 Essentially Yours: The Protection of Human Genetic Information in Australia

41 See, for example, HealthConnect Business Architecture v1.9 page 167 available at
The Australian Compliance Institute (16) submits, in regard to privacy regulation generally, that ‘as each State introduces new legislation, legal costs are incurred in understanding any potential impact’.

In regard to health privacy specifically, the Law Council of Australia (36) states that:

‘...increased compliance costs are incurred, particularly by organisations operating in more than one state or territory, which costs will be passed on to the consumer’.

The Pharmacy Guild of Australia’s (93) submission concurs with this view, noting also that many pharmacies may be small businesses (though they are still regulated by the Privacy Act because they handle health information and provide a health service).

A practical problem was identified in a stakeholder forum. A national medication service operating via a call centre must read different statements to obtain consent depending on the location of the individual (and the law that applies in that jurisdiction).

The Insurance Council of Australia (59) notes that these compliance costs may be incurred by any organisation which handles health information.

Forum shopping

A submission from a not-for-profit organisation (11) notes that ‘...potential complainants/plaintiffs [may] 'shop around', to select the most suitable legalisation to further their case or grievance’.

This view is supported by the Mental Health Privacy Coalition (58) which states that:

‘...small differences also allow legal practitioners the avenue towards arguing different aspects of privacy law in different jurisdictional legal settings, thus creating unnecessary headaches for healthcare providers’.

Confusion about which law to apply

A number of submissions contest that multiple privacy regimes create confusion for providers and consumers. Comcare (12) submits that:

‘our assessment is that some health professionals are unsure as to which privacy regime they are subject to when dealing with information relating to people in the Commonwealth jurisdiction’.

However, it also notes that ‘having said that, the incidence of this issue does seem very low.’
The Mental Health Privacy Coalition (58) submits that ‘a plethora of different laws or guidelines tends to confuse the health sector’. The AMA (29) states that ‘the mish-mash of privacy and health specific privacy legislation is confusing to both doctors and their patients’. A number of other submissions concur that the current arrangements create confusion\(^{42}\).

**Individuals uncertain about enforcing rights**

The Insurance Council of Australia (59) notes that multiple privacy regimes affect the ability of individuals to exercise their rights, as individuals need to be aware of the range of bodies to which they may seek recourse.

The Law Council of Australia (36) has expressed the view that “consumers are less likely to be able to clearly understand their rights in any particular situation and are likely to experience increased difficulty and frustration in enforcing those rights”.

The Australian Nursing Federation (ANF) (127) has submitted that there is consumer uncertainty about their rights, at least partly due to the exemptions in the Privacy Act, particularly the small business exemption, the employee records exemption and the journalism exemption.

In addition, the ANF (127) also holds that ‘general confusion exists regarding complaints processes’. Other submissions concluded also that multiple privacy regimes contribute to consumer uncertainty, as consumers may be unsure which regulator to complain to, and which law applies to their matter\(^{43}\).

A confidential submission refers to the ‘inequitable’ situation where individuals in some states can access their health information regardless of its collection date, but others can access only information collected after 21 December 2001 (the commencement date of the private sector provisions).

The Royal District Nursing Service of Melbourne (78) submits that while there appears to be adequate awareness of privacy rights in the general community, there ‘…is some difficulty in the awareness or understanding of the elderly’.

**Options for reform**

**Adoption of the proposed National Health Privacy Code**

Submissions support the work of the National Health Privacy Working Group in developing the proposed National Health Privacy Code. Adoption of the

\(^{42}\) Relevant submissions include AMA (29), Australian Government Department of Health and Ageing 99 and Australian Nursing Federation 127.

\(^{43}\) Relevant submissions include the AMA (29), SA Department of Health (95).
code by all jurisdictions would promote national consistency in the handling of health information.

The success of a national code will depend critically upon how it is implemented. Achieving consistency would involve all jurisdictions implementing the code unamended and in the same manner.

Therefore, one option is for each jurisdiction to incorporate the agreed code, as is, within its laws. The manner for legislatively enabling the code would also need to be the same in each jurisdiction.

**Code to be adopted as a Schedule to the Privacy Act**

For the Australian Government jurisdiction, the code could become a Schedule to the Privacy Act. The Schedule would apply the code to those bodies already within the jurisdiction of this legislation and that handle health information; that is, many Australian Government agencies and a range of private sector organisations.

This step could occur whether or not all jurisdictions adopt the proposed code. However, it is preferable that this step by the Australian Government is mirrored by each jurisdiction.

The need to ensure that the code is reflected in the Privacy Act is noted by the Victorian Health Services Commissioner (27). Similarly, the National Health and Medical Research Council (32) recommends that ‘a single, simplified national health privacy regulatory scheme’ (that is, the code) should replace and not supplement existing regulatory arrangements. The Australian Nursing Federation (127) highlights the importance of consistency between the Privacy Act and the code, and looks forward to a national regulatory framework that incorporates ‘a national process for [addressing] complaints and breaches’.

Once the code is adopted into the Privacy Act (particularly if as a schedule), the Australian Government could seek agreement from all jurisdictions for any subsequent regulatory measures in this area by them to be consistent with these provisions.

The code, as established through the Privacy Act, could become the de facto national standard for health privacy. If agreed, all other jurisdictions would be expected to adhere to this standard. Through this approach, the Australian Government would provide national leadership in this complex area. Success, however, again depends upon agreement by all jurisdictions.

**Code to be adopted by amending the NPPs**

Similar to the previous option, whether or not all jurisdictions adopt the code in the same way, the NPPs in the Privacy Act could be amended to ensure consistent privacy protection for Australian Government agencies and private
sector organisations that handle health information. The NPPs would be amended to incorporate the provisions of the code.

This approach would entail one set of privacy principles to regulate the handling of health information. These principles would be based on the NPPs, and include the provisions of the code. This would go some way toward addressing broader national consistency issues identified in this report; such as the differences between the IPPs and the NPPs.

However, the resulting principles would be longer and more complex. This option would require the insertion of multiple sub-principles and exceptions to the NPPs to take account of the code.

This approach would run counter to the intent of delivering general, high-level principles for all business and government sectors. For instance, the approach would mean that non-health organisations and agencies would need to deal with a more complex set of privacy principles, where much of the content may not apply to them. This would not improve, and may even increase, regulatory complexity overall.

**Stakeholder awareness and education**

If national consistency is pursued by legislative or regulatory intervention, and whether or not it is fully achieved, substantial awareness and education programmes could be developed to explain how the various privacy regimes interact.

This approach would involve providing awareness and education for consumers, providers and other stakeholders about the roles of the various schemes, the differences between them, and how to assert rights or to comply with obligations. The approach could reduce perceived uncertainties surrounding which laws apply to various organisations and agencies, including which complaint handling arrangements would operate. It would seek to assist stakeholders to work their way through the multiple and interacting privacy schemes.

This is likely to be resource intensive, not only for the Office and those in the Australian Government jurisdiction, but for state and territory agencies with regulatory and education/awareness responsibilities, and for private sector professional entities. It would not resolve national consistency issues (or the lack thereof) at law, nor would it create assurances about how health privacy laws interact.
### 2.6 Recommendations: Health Consistency

<table>
<thead>
<tr>
<th>Recommendation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>12</td>
<td>The Office urges the National Health Ministers’ Council to finalise the National Health Privacy Code. This should include agreement by all jurisdictions on the contents of the code and on its consistent implementation in each jurisdiction.</td>
</tr>
<tr>
<td>13</td>
<td>The Australian Government should consider adopting the National Health Privacy Code as a schedule to the Privacy Act. This would recognise the Australian Government’s part in the consistent enabling of the Code. Should agreement not be reached by all jurisdictions about implementing the Code, the Australian Government should still consider adopting the code as a schedule to the Act to provide greater consistency of regulation for the handling of health information by Australian Government agencies and the private sector. (See also recommendations 29, 33 and 35.)</td>
</tr>
</tbody>
</table>
2.7 Residential tenancy databases

What are residential tenancy databases?

Residential tenancy databases are privately owned electronic databases that contain information on the tenancy history of tenants. Property managers and landlords use them to assist in assessing risk and identifying potential problem tenants during the rental application process. Most property managers and real estate agents routinely subscribe to at least one tenancy database to screen prospective tenants. There do not appear to be industry standards or codes of practice which apply to them.

Application of the Privacy Act

The Privacy Act applies to tenancy databases with an annual turnover of more than $3 million. They also apply to tenancy databases with a turnover of $3 million or less, despite the small business exemption, because they trade in personal information. If, however, a tenancy database that is a small business, gains consent for the collection or disclosure of an individual’s personal information, then the Privacy Act does not apply.

Issues

There is a wide range of concerns about how tenancy databases operate. This section of the report is not concerned with the substantive issues. It is concerned only with the national consistency issues.

Tenancy databases are regulated by the Privacy Act and state and territory privacy legislation, including specific legislation regulating tenancy databases in some jurisdictions. Queensland and New South Wales have introduced legislation to prescribe listing and notification practices, and dispute resolution frameworks, and the ACT has foreshadowed similar legislation.

The Real Estate Institute Australia (13) draws attention to the lack of consistency in the various legislation, federal and state and territory, relating to tenancy databases. As this impacts negatively on consumers and business, the Institute suggests that a nationally consistent framework, with guidelines, should be developed for the operation of tenancy databases.

Options for reform

Australian Government could regulate tenancy databases

Tenancy databases operate nationally. The issues addressed by state and territory legislation are not confined to those states and territories, but are
national. A patchwork of legislation is emerging and adding to the lack of national consistency in privacy protection. The Australian Government could regulate residential tenancy databases.

**Commissioner could make a binding code**

Earlier in this chapter, the Report recommends that the Australian Government should consider amending the Privacy Act to give the Privacy Commissioner a power to make binding codes. One of the policy reasons for doing so is that there may be some business activities that give rise to issues that demand a regulatory response on a national basis. In the absence of federal legislation or uniform, or at least consistent, state and territory legislation, and assuming that the Australian Government amends the Act in accordance with the recommendation, the Privacy Commissioner could make a binding code to apply to residential tenancy databases.

**MCCA/SCAG process**

In August 2003, the Ministerial Council on Consumer Affairs (MCCA) and the Standing Committee of Attorneys-General (SCAG) agreed to establish a joint working party to consider residential tenancy databases. The Office is represented on the working party, which is chaired by the Attorney-General’s Department of the Australian Government. The working party intends to report to MCCA and SCAG by the middle of 2005. The Australian Government could make this process a matter of high priority.

**2.8 Recommendations: Residential tenancy databases**

| 14 | The Australian Government should advance as a high priority the work currently being undertaken by the Working Group on Residential Tenancy Databases of the Ministerial Council on Consumer Affairs/Standing Committee of Attorneys-General. |
| 15 | The Australian Government should consider, depending on the outcome of the Ministerial Council on Consumer Affairs/Standing Committee of Attorneys-General, making the Privacy Act apply to all residential tenancy databases. This could be done by using the existing power under section 6E to prescribe them by regulation, or by amending the consent provisions (section 6D(7) and section 6D(8)) that apply to the small business exemption. (See recommendation 53.) |
| 16 | If the Privacy Act is amended to provide for a power to make a binding code, (see recommendation 7), and depending on the outcome of the Ministerial Council on Consumer Affairs/Standing Committee of Attorneys-General, the Privacy Commissioner could make a binding code that applies to tenancy databases. |
3 International issues and obligations

3.1 EU Adequacy and APEC

Law and Policy

EU adequacy a driver of the legislation

An object of the private sector provisions was to ensure that Australia would be able to meet international obligations and not be disadvantaged in the global information market. The provisions aimed to provide adequate privacy safeguards to facilitate further trade with the European Union (EU). In the absence of the new provisions, the Explanatory Memorandum stated:

‘there are serious questions surrounding the ability of Australia to meet the requirements for continued trade with EU members under the European Union Directive on the Protection of Individuals with regard to the Processing of Personal Data and on the Free Movement of Such Data’\(^{44}\).

Privacy Act is not yet EU ‘adequate’

Negotiations with the European Commission regarding the adequacy of the Privacy Act in meeting the EU Directive have been continuing. The amendments to the Privacy Act in April 2004 were a result of these discussions\(^{45}\). These amendments to the legislation make it clear that the protection provided by NPP 9, which regulates transborder data flows, applies equally to the personal information of individuals who are Australian and those who are not. They remove the nationality and residency limitations on the power of the Privacy Commissioner to investigate complaints relating to the correction of personal information. They also give businesses and industries greater flexibility in developing privacy codes by allowing the codes to cover otherwise exempt acts and practices where the authors of the code wish to do so. However, there are ongoing discussions with the European Commission regarding the small business and employee records exemptions from the Privacy Act.

The EU has not granted Australia ‘adequacy status’ regarding the EU Directive nor has it stated that Australia’s privacy regime is inadequate. At this stage, the EU has declared Switzerland, Canada, Argentina, Guernsey, Isle of Man, the US Department of Commerce’s Safe Harbour Privacy Principles, and the transfer of Air Passenger Name Record to the United

---

\(^{44}\) Privacy Amendment (Private Sector) Bill 2000 Revised Explanatory Memorandum – Senate, November 2000, p11.

\(^{45}\) Privacy Amendment Act 2004.
States' Bureau of Customs and Border Protection as providing ‘adequate’ privacy protection.

Asia-Pacific Economic Cooperation (APEC) framework

The endorsement of the APEC Privacy Framework by APEC Ministers in November 2004 means that APEC countries, including Australia, need to make sure that their privacy regimes meet a new set of international obligations. The APEC privacy framework has a number of aims including promoting electronic commerce, providing guidance to APEC economies and helping to address common privacy issues for business and consumers in the region. The initiative has the potential to accelerate the development of information privacy schemes in the APEC region and to assist in the harmonisation of standards across national jurisdictions.

The APEC framework, like the NPPs, was designed to be consistent with the core values of the Organisation for Economic Cooperation and Development’s (OECD) 1980 Privacy Guidelines. The APEC Principles cover areas such as notice, collection, use and disclosure, choice, integrity of personal information, security safeguards, access and correction and accountability. APEC will continue making decisions about the implementation of the APEC principles during 2005.

Issues

The issues paper noted that it was not clear whether organisations are finding that their commercial activities are impeded by the private sector provisions in their current form. It raised issues such as whether the private sector provisions are working for businesses in relation to their global operations and whether they will work in the future and what strategies businesses are using to deal with any issues that are arising, for example, using contractual provisions.

What submissions say - issues

Lack of EU adequacy has not inhibited trade

One submission (confidential) says the Privacy Act does not seem to resolve the question of whether privacy laws meet the standards of international obligations. Nevertheless, only a very small proportion of the submissions that the Office received from stakeholders and few of the comments made in consultation meetings indicate that the failure to achieve EU adequacy has impaired business and trade with European organisations. One confidential submission, for example, raised concerns that Australian organisations are unable to state that their privacy policies actually meet contractual obligations.

---

46 APEC Privacy Framework 29 October 2004, p3
47 See for example Australian Information Industry Association 43
of international agreements. On the other hand, the Australian Direct Marketing Association (67) states:

‘it is clear that although Australia’s privacy regime has not been recognised as ‘adequate’ for the purposes of the EU this has not hindered organisations’ ability to conduct business with European counterparts’48.

The Australian Bankers Association (70) and the Investment and Financial Services Association Ltd (89) call for the Privacy Commissioner to press for EU adequacy.

3.2 Recommendation: EU ‘adequacy’ and APEC

17 There is no evidence of a broad business push for ‘adequacy’. Given the increasing globalisation of information, however, there may be long term benefits for Australia in achieving EU ‘adequacy’. Certainly the globalisation of information makes the implementation of frameworks such as APEC important. The Australian Government should continue to work with the European Union on the ‘adequacy’ of the Privacy Act and to continue work within APEC to implement the APEC Privacy Framework.

3.3 NPP 9

Law and policy

The operation of NPP 9 is an important aspect of the global operation of the private sector provisions. NPP 9 outlines the circumstances in which an organisation can transfer personal information it holds to other countries. This principle is based on the restrictions on international transfers of personal information set out in the European Union Directive 95/46.

In its simplest terms, NPP 9 prevents an organisation from disclosing personal information to someone in a foreign country that is not subject to a comparable information privacy scheme, except where it has the individual's consent or some other circumstances apply including where:

- the transfer is for the benefit of the individual and the organisation can show grounds for a belief that if it were practicable to obtain consent the individual would be likely to give it or

48 Australian Direct Marketing Association 67
• 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.

NPP 9 does not prevent transfers of personal information outside Australia by an organisation to another part of the same organisation, or to the individual concerned. On the other hand, a company transferring personal information overseas to a related company must comply with NPP 9.

Issues

The issues paper noted that it is not clear how easy or otherwise organisations are finding it to work with the provisions of NPP 9 when transferring information, or the extent to which organisations are complying with NPP 9.

What submissions say - issues

Related companies

The Law Council of Australia (36) and the Investment and Financial Services Association Ltd (89) call for clarification in the way NPP 9 and section 13B(1) operate together. These submissions argue that it is not clear whether section 13B(1) enables a body corporate in Australia to transfer personal information to a related body corporate located outside of Australia without reference to NPP 9. One confidential submission states that transfer between related companies should not require additional consent.

Establishing a law is substantially similar

Comments made during the consultation process indicate that there are a number of problems faced by organisations in respect to NPP 9. Many stakeholders express frustration at the fact that there is a lack of guidance regarding the countries whose regimes provide adequate protection equivalent to the NPPs49. In this situation the onus is on the organisation to assess the regime of the country in which their trading partner resides. Many stakeholders, especially small businesses, have criticised the efficiency of this system arguing that they neither have the expertise or the resources to assess a foreign country’s privacy laws.

Contract

From submissions and the comments received during stakeholder workshops, it appears that organisations are fulfilling their NPP 9 obligations of ensuring that personal information is protected when it is transferred to regions without

49 See for example Association of Market Research Organisations and Australian Market and Social Research Society 61; Telstra Corporation Ltd 110; ANZ 40; Confidential Submission
privacy regimes through contractual arrangements with their trading partners\textsuperscript{50}. While some submissions find this to be an effective solution\textsuperscript{51}, others are concerned about the costs associated with monitoring the compliance of their trading partners\textsuperscript{52}.

**Other Issues**

During stakeholder consultations, many consumers expressed concerns about overseas call centres\textsuperscript{53}. The recent growth of international call centres has also attracted some attention in the media. The transfer of personal information overseas brings with it a perceived loss of privacy and control.

**What submissions say - addressing the issues**

**Publish a list of countries with adequate privacy regimes**

It has been suggested during consultations that the Privacy Commissioner should publish a list of countries found to have adequate privacy regimes\textsuperscript{54}. Coles Myer Ltd (60) argues that publishing such a list would require the Commissioner to review and rate laws and governmental directives beyond privacy legislation which would need to be constantly updated. Coles Myer Ltd (60) does not recommend the Commissioner’s resources be used on NPP 9.

**Greater guidance**

Some submissions suggest that the Office could provide greater guidance through publishing approved standard contracts to be signed by Australian companies and international trading partners which include provisions that protect information collected in Australia when it is transferred to organisations overseas\textsuperscript{55}. The Australian Direct Marketing Association (67) states that an information sheet outlining the issues that should be addressed as part of a contractual agreement would also be beneficial.

**Require notice that information sent overseas**

Electronic Frontiers Australia (51) argues that the NPPs should be amended to require organisations give individuals notice that their information will be sent to a foreign country and that the individual will be required to deal with call centres located in a foreign country. Electronic Frontiers Australia (51)

\textsuperscript{50} Coles Myer Ltd 60; Australian Direct Marketing Association 67; Telstra Corporation Ltd 110; Australian Bankers Association 70
\textsuperscript{51} For example Telstra 110; Australian Direct Marketing Association 67; Coles Myer Ltd 60
\textsuperscript{52} Confidential Submission.
\textsuperscript{53} See also Electronic Frontiers Australia Inc 51.
\textsuperscript{54} Association of Market Research Organisations and Australian Market and Social Research Society 61; Telstra Corporation Ltd 110; ANZ 40; Confidential Submission.
\textsuperscript{55} This is an approach favoured by Australian Direct Marketing Association 67; Australian Bankers’ Association 70; Confidential Submission.
also supports requiring organisations to notify individuals of the means by which the Australian organisation has ensured their personal information will be adequately protected, unless the overseas organisation is subject to substantially similar privacy laws or the individual has consented to the transfer.

**Options for reform**

Exclude related companies from complying with NPP 9

Disclosure of personal information about an individual by a body corporate to a related body corporate is not ‘an interference with the privacy of an individual’ under section 13B(1)(b). Section 13B relates to the purposes for which information can be disclosed. NPP 9 on the other hand relates to whether or not information can be sent overseas. As section 13B(1)(b) enables disclosure of information, compliance with NPP 9 for transfers of information to a foreign country is still required.

If a company has an organisational link with Australia under section 5B, the extra-territorial provisions in the Privacy Act will apply. Therefore, if personal information is sent overseas to the same company, it will continue to be protected by the Privacy Act because the extra-territorial provisions apply. Section 5B does not appear to apply to related entities outside of Australia. As such, if information is sent to a related company, it may not be protected by the Privacy Act.

Where information is transferred outside of Australia and the extraterritorial provisions do not apply, it is in the public interest that NPP 9 applies. NPP 9 ensures that once the information is transferred, it will be treated in a way that is consistent with Australian privacy laws, or in a way in which the individual consents. The Office does not recommend excluding related corporations from NPP 9.

Publish a list of countries with substantially similar laws

Publishing a list of countries with substantially similar privacy laws would give organisations that transfer information overseas certainty about the countries to which they can safely transfer information. Establishing whether laws are substantially similar is, however, a very complex task. It would require considerable resources and would have implications for our relationships with other countries. It is not clear that this is an appropriate role for the Office.

Publish standard contractual provisions

The Office could provide greater guidance through publishing approved standard contractual provisions for use by Australian companies and international trading partners. These contractual provisions could provide for how the international company must protect information when the information collected in Australia is transferred to organisations overseas. The EU has
issued contract provisions. Developing standard contractual provisions would have resource implications for the Office.

Provide greater guidance through information sheet

The Office could provide greater guidance through publishing an information sheet that outlines the types of issues that should be addressed as part of a contractual agreement and how to more easily assess whether a privacy regime is substantially similar. Although still resource intensive, this may be a more practical approach to take than issuing standard contractual provisions.

3.4 Recommendation: NPP 9

18 The Office will provide further guidance to assist organisations comply with NPP 9 by issuing an information sheet outlining the issues that should be addressed as part of a contractual agreement and how to more easily assess whether a privacy regime is substantially similar.
4 Protecting individual’s right to privacy

4.1 Control over personal information

Law and policy

The NPPs reflect the policy that an individual should generally know what personal information an organisation has about him or her and how it intends to use it. The organisation must not collect information unless it is necessary for one or more of its functions or activities (NPP 1). Whether the information is collected directly from the individual or indirectly from a third party, the organisation should ‘take reasonable steps’ to tell the individual, among other things, the purposes for which the information was collected, to whom the organisation usually discloses such information and the consequences of not providing it (NPP 1.3 and NPP1.5).

Generally speaking, the organisation cannot use or disclose the information for a purpose other than that for which it was collected (a secondary purpose) unless:

- the purpose is related (or directly related if the information is sensitive information) to the primary purpose and the individual would reasonably expect the organisation to use it for such a purpose or
- the individual has consented to the use or disclosure (NPP 2.1).

The NPPs apply to the collection of personal information for inclusion in a generally available publication, such as a telephone directory. They do not apply, however, once the information has been collected.

Issues

Possible topics for submissions

The issues paper suggested possible topics for submissions. They are:

- extent to which organisations are adopting a bundled consent approach to their information handling practices
- collection practices that limit an individual’s control over his or her personal information
- extent to which current practices are essential to business efficiency that outweighs the impact on individual privacy interests
- effectiveness of NPPs in ensuring consent to use and disclosure of personal information, where required, is real and voluntary, or if not possible, measures needed to compensate for not having a chance to give real consent
- extent to which it should be possible for individuals to consent to unrelated secondary purposes
- issues arising in relation to the private sector provisions and personal information that is publicly available and
- ways of overcoming any issues that arise on this topic.

**Information collected indirectly**

The issues paper noted that it may be more difficult to ensure the individual is aware of the matters listed in NPP 1.3 and NPP 1.5 when the organisation collects personal information indirectly. It acknowledged that in some cases it may be ‘reasonable’ to make less effort to give people NPP 1.3 information than it would otherwise be, or even to do nothing at all.

If the individual is not informed, however, he or she may have lost the control over personal information that the NPPs intended individuals should generally have. Information given to one organisation (compulsorily in the case of some publicly available information) may be used by another organisation for a completely different purpose without the individual’s knowledge.

**Bundled consent**

The issues paper noted that the NPPs do not specifically require organisations to get an individual’s consent to collect personal information (except sensitive information). An organisation can use and disclose personal information without consent as long as the use or disclosure is for the main purpose of collection, or a related (or directly related in the case of sensitive information) purpose and is within the individual’s reasonable expectations. Generally speaking, an organisation need only get an individual’s consent for uses and disclosures of personal information that are for unrelated secondary purposes.\(^{56}\)

The issues paper focussed on bundled consent, that is, the bundling together of consent to a wide range of uses and disclosures of personal information without giving the individual an opportunity to choose which uses and disclosures they agree to and which they do not, often sought as part of the terms and conditions of a service.

**Community attitudes survey**

The Office commissioned research into community attitudes towards privacy in 2001 and 2004\(^7\). *Community Attitudes Towards Privacy 2004*, reports that while the quality of a product or service was rated as the most important

---

56 See NPP 2 generally but also NPP 2.1(c), which allows use for the unrelated secondary purpose of direct marketing without consent in certain circumstances.

57 See Appendix 6.
element of customer service by respondents, respect for and protection of personal information was rated almost as highly.

The survey also reports that privacy policies are not necessarily being read, partly due to the length and complexity of the information. Respondents were asked what aspects of privacy policy are most important to be included in a short privacy notice. The order of importance is:

- how the information will be used (47%)
- if and when the organisation will pass on my information (15%)
- what information will be kept (15%)
- how to prevent being contacted for marketing purposes (12%)
- how to access or change my information (6%)
- can’t say (4%).

What submissions say - issues

Collection practices

Submissions raise a number of issues arising from the collection of personal information. In the view of the Australian Privacy Foundation (90), there is widespread non-compliance with the requirements of NPP 1.3 and NPP1.5, which will not be likely to be exposed by complaints. Nevertheless, it is satisfied with the qualification that an organisation take ‘reasonable steps’ to ensure that the individual is aware of the matters listed in NPP 1.3.

An organisation’s functions or activities

NPP 1.1 limits the collection of personal information by an organisation to that necessary for its ‘functions or activities’. The organisation itself, however, determines what its functions and activities are and the limitation on the collection of information may be seen to be illusory.

A number of participants in stakeholder forums raised the issue of the collection of unnecessary personal information. It was said, for example:

- when real estate agents collect personal information from tenants, the tenant has little choice but to give the agent the information, otherwise the agent may not deal with them
- there are problems with the extent of health information sought as part of pre-employment checks
- insurers also sometimes seek more information than seems to be necessary and
- a charity organisation said it could not afford to oppose a subpoena demanding access to its files.
Privacy notices

It was suggested that some NPP 1.3 and 1.5 notices are unhelpful and confusing and probably do more harm than good in terms of public awareness and understanding. The Law Council of Australia (36) notes that a practice has emerged of organisations providing lengthy privacy collection notices. It believes organisations are trying to address the criteria required by NPP 1.3 and to put individuals on notice as to what uses and disclosures they might reasonably expect. As a result, it says, consumers are confused.

Electronic Frontiers Australia Inc (51) expresses concern about the practice of including NPP 1.3 information in privacy policies that are subject to change without notice and often are not dated. It provides examples of such notices, including:

[Mobile phone company] reserves the right to change this Privacy Policy at any time and notify you by posting an updated version of the Policy on its web site. The amended Privacy Policy will apply between us whether or not we have given you specific notice of any change. We encourage you to review this Privacy Policy periodically because it may change form time to time.

Confusion about who should notify

Another issue is the question of who should be responsible for notifying the individual when personal information is rented or sold by one organisation to another: the organisation that collected the information in the first place, or the organisation to whom it has been sold for use. Australia Post (109) and two confidential submissions address this issue.

Indirect collection

Finally, the Australian Consumers Association (15) raises the issue of indirect collection. It is concerned that an individual has no control when personal information is collected indirectly. The collector may collect the information for a primary purpose quite unrelated to the individual’s expectations when he or she handed over the information in the first place:

‘Many of the ‘protections’ in the Act revolve around the control of secondary uses of personal information. However indirect collection can have a primary purpose unrelated to the consumers’ expectations when the data was originally given up – and hence the data is magically transmuted into information the use and possession of which at best the consumer can expect to be informed in retrospect.’
**Bundled consent - consumer viewpoint**

Most submissions that address the issue of consent discuss bundled consent. The submissions fall into two categories. Submissions from consumer groups are highly critical of the practice of bundling consent. Submissions from business organisations say why it is necessary.

‘Bundled consent’ refers to the practice of bundling together consent to a wide range of uses and disclosures of personal information without giving individuals an opportunity to choose which uses and disclosures they agree to and which they do not. Many submissions address the issue. Submissions from consumer groups criticise the practice.

The Australian Consumers’ Association (15) describes it as ‘where consent is sought too broadly for the consent to have any real controlling influence on the relationship the consumer has with the business.’ Xamax Consultancy Pty Ltd (3) says that it totally undermines the requirement that consent be meaningful, informed and freely given.

In the view of Electronic Frontiers Australia Inc. (51), individuals cannot give free and informed consent when they are presented only with broad and/or vague statements concerning possible uses and disclosures, and/or told that services will not be provided if they do not ‘consent’ to the bundle.

The Consumer Credit Legal Centre’s (62) submission includes a case study highlighting a credit contract which included the statement:

> 'I hereby authorise [Finance Corp] or their agents or employees to discuss any information about my account with anyone (emphasis added).’

Some insurers insist members sign a release form allowing the insurer to access any of their records at any time for any reason. The Australian Physiotherapy Association (37) says that this is inappropriate for sensitive health information. It also identifies another unacceptable practice, namely the use of bundled consent by third party insurers to obtain information, sometimes years after the treatment.

The Australian Communications Authority (94) is concerned that individuals are not given the opportunity to consent to some uses and not to others. It says that denial of service is common and that organisations also bundle the receipt of commercial electronic messages from the organisation itself or others with delivery of service or membership arrangements. It is not, in its view, good practice to make provision of a service or other benefits conditional on consent to receive commercial electronic messages.
The Australian Privacy Foundation (90) distinguishes between bundling consent to use or disclosure for a variety of purposes, which may be reasonable in some circumstances, and making consent for a non-essential secondary purpose a condition of doing business, which is not.

**Bundled consent - business viewpoint**

Many submissions from business, in particular the finance and telecommunications industries, outline the reasons why it is often necessary to bundle consent. Submissions from the health sector also address this issue.

**Telecommunications**

Both Virgin Mobile (Australia) Pty Ltd (26) and Vodafone Australia Ltd (112) state that obtaining consent for each specific use of an individual's personal information would significantly increase the complexity and the costs of compliance. Virgin says that these costs would inevitably be passed on to consumers. Furthermore, says Vodafone, unbundling consent would result in an undesirable customer experience for both consumers and suppliers because of the increased volume and frequency of communications that would be necessary to achieve the same result that bundled consent achieves more efficiently.

**Finance**

Submissions from the finance industry explain why, in the industry's view, bundling consent is necessary. The Australian Finance Conference (AFC) (63) states that bundled consents have arisen because the meaning of 'primary purpose' is uncertain. 'Primary purpose' can be interpreted narrowly or broadly. When a customer submits an application for finance, it asks, is the processing of the application the primary purpose of collection, or is it, more broadly, the provision of finance. If the latter, it would include, in addition to processing the application, managing the account, administering insurance claims, recovering money owed and maintaining the value of the asset. The Investment and Financial Services Association Ltd (89) makes a similar point. Both submissions state that to require individual consents for each process would be very costly. In the view of the AFC (63):

'It was not Parliament’s intention that a financier should be obliged to separately identify each of these uses and provide the individual with the option of selecting which of them he or she consents to. While a computer program could be designed to implement this the cost would be prohibitive and the daily management of customer choices virtually impossible.'
The AFC (63), the Australian Bankers Association (70) and Suncorp Metway Ltd (35) identify other reasons relevant to the issue of bundled consent in the finance industry. For example, the banker's duty of confidentiality and motor vehicle licensing and registration may require a disclosure notification beyond that required by the Privacy Act. Banks outsource many of their functions to service providers, many of whom are offshore, and if a customer failed to consent to the disclosure of their information to the service provider it would be unlikely that the organisation could provide a service to the customer. Finally, they say customers have extensive freedom and choice of product and provider in the finance sector.

**Doctors**

The Australian Medical Association Ltd (29) states that doctors will continue to bundle consent as long as the primary purpose for collecting personal information in NPP 2 is taken to relate to an episode of care. If, on the other hand, primary purpose were the health and well being of the patient then there would be no need for doctors to bundle a series of consents. In addition, in the view of the Department of Health, South Australia (53) it is impractical not to have bundled consent in the context of existing electronic architecture and general medical practices, and that it is impractical to make a decision in one sector (for example, the private health sector) because it will inevitably affect the other because of the interconnectedness of the public and private medical sectors.

**Residential tenancy databases**

Residential tenancy databases are a particular case. Many real estate agents use tenancy databases to help them decide whether or not to let a property to a particular person. When applying to rent a property a prospective tenant will be expected to provide personal information for disclosure to a tenancy database. He or she has little choice but to consent. The Tenants' Union of Queensland (69) says:

‘Through one signature, individuals’ consent is gained for a range of matters, and without this they will be denied the tenancy. By gaining this consent, the collecting organisation has a greater ability to use and disclose the information. The uneven bargaining power means consumers have little or no power to resist the invasion of privacy and are pressured to consent to a range of things they may not really agree with’.

The Tenants' Union ACT (87) agrees. It believes that, because of this practice, a prospective tenant has no real choice about handing over their personal information, so the protection that would otherwise be provided by the NPPs is lost to them, that is, the NPPs do not work.
At recommendation 7, this report suggests that the Australian Government should consider amending the Privacy Act to provide for a power to make a binding code. It also recommends that, assuming the Act is amended, the Commissioner could make a binding code that applies to tenancy databases. (See recommendation 16 in Residential Tenancy Databases section.)

**Publicly available information**

Many people are uncomfortable with the notion that publicly available information, including the electoral roll and the white pages, can be used for purposes other than those for which the information was collected. In the survey, *Community Attitudes towards Privacy 2004*, commissioned by the Office, for example, 77% of respondents thought that the electoral roll should not be used for direct marketing and 46% thought that the white pages should not be. The issue is more critical as technological developments make it easier to manipulate the material, for example, by reverse sorting it to identify a person's address from their telephone number.

Submissions are divided as to whether or not publicly available personal information should be subject to the NPPs. Some, for example, Xamax (3) say that publicly available information should be used only for the purpose for which it was collected. The Australian Privacy Foundation (APF) (90) urges the reconsideration of the breadth of the exemption of publicly available information from the operation of the NPPs, other than the collection principles.

The Australian Communications Authority (94) states that the use of publicly available information should be conditional so that 'it is not automatically assumed an individual agrees to it being used for a myriad of purposes simply as a result of it being readily available'.

Charities are of the opinion that access to generally available information is necessary in order to raise funds. According to the Cerebral Palsy League of Queensland (44), ‘access to publicly listed information is the key to the survival of many organisations’. Not having access would limit its ability to raise funds and to assist in providing services to people with cerebral palsy.

Some businesses use publicly available personal information to cleanse their data. Coles Myer (60) is concerned that access to public registers is diminishing as they are ‘a valuable tool to ensure data quality and accuracy obligations under the Privacy Act are met.’ In the view of the Australian Direct Marketing Association (ADMA) (67), the industry would struggle to maintain current levels of accuracy without publicly available information, which it regards as an ‘essential updating and validation tool’.

---

58 See also Scope 68.
59 NPP 3 provides that an organisation must take reasonable steps to make sure that the person information it collects, uses or discloses is accurate, complete and up-to-date.
For members of the Australian Finance Conference (63), it is imperative to be able to continue to collect personal information from public sources to verify objectively the identity of an applicant for finance and his or her asset holdings, and to confirm capacity to repay. They believe also that access to public sources is essential to meet their obligations under NPP3.

The Australian Institute of Private Detectives (38) and the Institute of Mercantile Agents, the Australian Collectors Association and the Australian Institute of Credit Management (115) argue in favour of the continued availability of publicly available information to enable them to carry out their investigative and debt collecting functions.

Finally, some submissions want no change to the existing law. Australia Post (109), for example, believes that any proposal to review the collection and use of publicly available personal information is unnecessary. Similarly, the Victorian Automobile Chamber of Commerce (113), whose members use publicly available personal information, among other sources, to identify potential customers, would oppose any proposal to prohibit or limit its use.

**What submissions say - addressing the issues**

**Short form privacy notices**

One of the consequences of the requirements of NPP 5 (Openness) and NPPs 1.3 and 1.5 is that privacy notices are often very long. In the view of Australia Post (109), the obligations imposed on organisations by NPP 5, particularly NPP 5.1 have had the positive effect of creating privacy awareness in the community.

The Law Council of Australia (36) supports the move by the Data Protection and Privacy Authorities internationally to develop a condensed or short privacy notice. Furthermore, it considers that organisations should not be required to include information which is obvious to the ordinary consumer in a privacy collection notice. The need for short privacy notices was also raised in consultations. On the other hand the Investment and Financial Services Association (89) says that although disclosure documents issued by its members may appear lengthy they contain detailed information assisting consumers to understand their rights.

**Office should give more guidance**

The Australian Privacy Foundation (90) suggests that further guidance from the Office as to what constitutes an acceptable NPP 1.3 or NPP 1.5 notice, or what does not, would be helpful. It also suggests the Office could play a role in improving the intelligibility and clarity of notices. It suggests the Office should become much more proactive in issuing template notices for different sectors and that these should be developed in consultation with industry bodies and relevant non government organisations.
Stricter regulation of privacy notices

Electronic Frontiers (51) suggests that privacy policies containing NPP 1.3 and NPP 1.5 information should have to include the date of issue and changes made since the earlier version should have to be highlighted or noted. It also suggests that changes to NPP 1.3 and NPP 1.5 information involving new uses or disclosures should not be able to apply to previously collected information, unless the organisation has directly notified the individual concerned of the changes and provided an opportunity to opt-out of the new uses or disclosures, or to terminate the relationship with the organisation without detriment.

Finally, Electronic Frontiers (51) suggests an organisation should not be able to rely on NPP 2.1 to use or disclose an individual’s personal information, unless the information in the NPP 1.3 or NPP 1.5 notice is specific enough to enable the individual to give free and informed consent, or to make and informed choice about whether to provide the information. A confidential submission also states that the notification requirements should be strengthened in the context of the transfer of health information within multidisciplinary teams.

Onus should be on supplier of personal information

A confidential submission states that list brokers and telecommunications companies that supply lists to other organisations should be required to ensure that their list collection and generation processes are compliant with NPP 1.3 and NPP 1.5 to reduce complaints to the organisations using the lists.

Limit collection

The Australian Privacy Foundation (APF) (90) suggests that, unless NPP 1.1 requires an objective test of what is necessary for an organisation’s functions or activities, that is, that the organisation cannot determine for itself whether or not information is necessary. It says NPP 1.1 should be amended to make it clear that compliance can legitimately be challenged by a third party, particularly by the person whose information is being collected.

APF (90) goes on to say that there should also be a proportionality requirement, that is, the type and amount of personal information collected should be no more than is required for the collector’s primary purpose. Consideration should also be given to including a provision that collection should be allowed ‘only for purposes that a reasonable person would consider are appropriate in the circumstances’60.

60 See Personal Information Protection and Electronic Documents Act 2000 (Canada) section 5(3).
The Australian Retailers’ Association (111) recommends that the collection of personal information for the purpose of making refunds should be explicitly allowed under the Act. This is because, it says, the ability to collect personal information when making a refund provides some degree of protection against a possible fraud where the goods have been stolen and exchanged for cash.

The Privacy Law Consulting Network (66) suggests that, in the light of the judgment in a case decided in 2004\(^\text{61}\), it would be desirable to define the phrase ‘functions or activities’ to provide more certainty for business.

**Publicly available personal information**

The Australian Finance Conference (63) recommends that the definition of personal information be amended to exclude information obtained from public sources and unsolicited information.

## Options for reform

### Amend NPP 1.1

NPP 1.1 limits the collection of personal information to that necessary for its ‘functions or activities’. This limitation could be strengthened by making the test of what is necessary for an organisation’s functions of activities an objective one. The organisation itself would not be the judge of what information is necessary. NPP 1.1 could be amended to make the test an objective one. This would make it possible for an individual to challenge the collection of particular information. However, in practice it would be difficult to implement. Furthermore, it is not likely that the benefits of doing so would outweigh the costs.

### Amend NPP 5.1

NPP 5.1 requires an organisation to set out in a document clearly expressed policies on its management of personal information. It is, however, somewhat vague about what it requires organisations to do. Short form notices would improve the quality of an organisation’s communication with its customers. NPP 5.1 could be amended to clarify the openness obligation.

### Privacy notices could be dated

Privacy notices are often not dated. This makes it difficult for consumers to establish exactly what he or she was told, or agreed to, at a particular time. Privacy notices could be dated as a matter of ‘best practice’, and the Office could publish an advice to that effect.

\(^{61}\) Seven Network v Media Entertainment and Arts Alliance [2004] FCA 637
Develop short form privacy notices

Privacy notices have become very long. A long privacy notice may not fulfil its purpose of informing a consumer because the consumer may be overwhelmed and confused because it is too long. The Office’s Community Attitudes Survey reports international research that shows that people do not necessarily read privacy notices, partly because they are too long and complex.\footnote{See Community Attitudes towards Privacy 2004, p 39.}

Longer privacy notices have come about partly as a result of organisations’ uncertainty as to the distinction between the primary and secondary purposes of collection and their attempt to avoid ‘bundling’ consent to a number of purposes of collection. There are international moves to develop short form privacy notices. There could be provision for short form notices, followed by a longer notice that includes all the information required by NPPs 1.3 and 1.5. A consumer who is satisfied with the information provided in the short form notice need not read the longer notice, yet all the information is available to the consumer who wants it. This may also satisfy the Openness requirement in NPP 5.

Office could assist organisations with notices

The Office is currently working towards developing a short notice for its own personal information handling practices with a view to demonstrating how such a notice might work in a public sector agency. It acknowledges that getting notices right may be difficult for some organisations, especially smaller businesses that do not have access to extensive legal advice. Subject to the availability of resources, the Office could play a more active role in assisting businesses develop their notices by developing template notices for different sectors, in consultation with them, and by issuing examples of both satisfactory and unsatisfactory notices.

Office could publish guidance on bundled consent

Bundled consent is a practice that may confuse consumers and may derogate from their rights under the Act. It is also an issue that confuses a lot of organisations. The Office could play a role in working with stakeholders to clarify the issue. The Office could publish guidelines about bundled consent.

Publicly available personal information

It is clear that restricting the use of publicly available personal information further than has already occurred may inhibit the operations of some businesses and the fundraising activities of charities. However, as currently applied, it is consistent with the policy underlying the Privacy Act that information provided for a purpose should be used only in accordance with that purpose.
Office could play greater educative role to raise community awareness

Community awareness of individuals’ privacy rights and confidence in the protection of individuals’ rights is growing slowly but is not high. The greater the awareness an individual has about his or her rights, the more likely he or she will exercise control over what is done with the information. The Office could play a significant role in raising community awareness and confidence. Business and consumer groups alike agree that this should be so. An enhanced educative role would have resource implications for the Office. This is discussed in more detail later in this chapter.

4.2 Recommendations: Control over personal information

19 The Australian Government should consider amending NPP 5.1 to provide for short form privacy notices. This could also clarify the obligations on organisations to provide notice, and to clarify the links between NPP1.3 and NPP 5.1.

20 The Office will encourage the development of short form privacy notices. It will also play a more active role in assisting businesses develop their notices by developing template notices for different sectors, in consultation with them, and by issuing example of both satisfactory and unsatisfactory notices.

21 The Office will develop guidance to the effect that privacy notices should be dated.

22 The Office will develop guidance on bundled consent, noting the possible tension between the desirability of short form privacy notices and the desirability of lessening the incidence of bundled consent.
4.3 Direct marketing

What is direct marketing?

Direct marketing refers to the promotion and sale of goods and services directly to the consumer. Direct marketers promote their goods and services by mail, telephone, email or SMS. They compile lists of consumers and their contact details from a wide variety of sources. These include public records, including the white pages, the electoral roll, registers of births, deaths and marriages and land titles registers. They also include membership lists of business, professional and trade organisations, survey returns, mail order purchase information and so on. Organisations that have their own database of consumers to whom they supply goods or services, for example, telephone companies and other utilities, may also use their database for direct marketing. Direct marketers may also acquire databases from other direct marketers.

Law and policy

When can personal information be used for direct marketing

Direct marketing is directly addressed by NPP 2.1, which governs the use and disclosure of personal information. NPP 2.1 distinguishes between the primary and the secondary purposes of collecting personal information, and limits the use and disclosure of information for a purpose other than the primary purpose of collection.

Information collected for the purpose of direct marketing

An organisation that collects information for the primary purpose of direct marketing, whether directly from the individual who owns the information or from someone else, can use and disclose it for that purpose. The same applies if direct marketing is related to the purpose for which the information was collected (directly related in the case of sensitive information) and the person from whom it was collected would reasonably expect the organisation that collected it to use or disclose it for direct marketing.

Information not collected for the purpose of direct marketing

In some circumstances an organisation can use personal information for direct marketing even if direct marketing was not the primary purpose of collection and direct marketing is unrelated to the purpose of collection and not within the reasonable expectations of the person who owns the information. The organisation may use the information if:
• the person from whom the information was collected has consented to the use or disclosure of the information for direct marketing or
• (if the information is not sensitive information) it is impracticable to get consent before using the information and
  o the direct marketing organisation gives the individual the opportunity to opt-out of receiving material (at no cost)
  o the individual has not already asked the organisation not to send material
  o in every communication the organisation draws the individual’s attention to the fact, or prominently display a notice, that he or she may opt-out of receiving further material and
  o each communication includes the relevant contact details of the organisation (including electronic contact details if the material was sent by electronic means)\textsuperscript{63}.

Individual may not know that information has been collected for the purpose of direct marketing

An individual whose information is collected by a direct marketing organisation for the purpose of direct marketing may not necessarily know that this has occurred. The organisation may, for example, purchase a list from another organisation. The purchasing organisation must then ‘take reasonable steps’ to ensure the individual has been made aware of, among other things, the purposes for which the information was collected\textsuperscript{64}.

Whether or not the individual is made aware hinges therefore on what constitutes reasonable steps to make him or her aware. It may be reasonable to do very little to ensure that all the people on the list are made aware that the list has been acquired for the purposes of direct marketing. Even when the information is collected from the individual directly he or she may not understand it is being collected for direct marketing purposes. For example, an organisation may run a competition for the primary purpose of collecting information; awarding prizes to successful entrants being a secondary purpose. The individual, on the other hand, may assume that the purpose of the competition is to provide an opportunity to consumers to win prizes. Even if he or she reads the fine print, an individual is unlikely to draw a distinction between a primary and a secondary purpose and to understand the consequences of the distinction.

**Rationale**

The provisions are intended to strike a balance between the business interests of organisations involved in direct marketing and the privacy interests of consumers affected by the activity. The legislation acknowledges the commercial practice of direct marketing and the related activity of acquiring personal information about individuals to enable organisations to

\textsuperscript{63} NPP 2.1(c).
\textsuperscript{64} NPP 1.5; NPP 1.3.
market their products efficiently and effectively. It also recognises the privacy interests of individuals who may find themselves the unwilling recipients of direct marketing material.

**Community attitudes survey**

The Office commissioned research into community attitudes towards privacy in 2001 and 2004. *Community Attitudes Towards Privacy 2004*, reports that concerns about unsolicited marketing material have dropped slightly since the 2001. Nevertheless, 61% of respondents feel either ‘angry and annoyed’, or ‘concerned’ when they receive marketing material. While 77% of respondents are opposed to the use of the electoral roll for marketing purposes, respondents are roughly evenly divided about the use of the White Pages (44% in favour and 46% against).

**Issues**

The issues paper drew attention to the fact that the NPPs require organisations to give individuals the opportunity to opt-out of receiving material when direct marketing is a secondary purpose of collection of personal information but do not do so when direct marketing is the primary purpose of collection. The issues paper suggested possible topics for submission, including:

- the appropriateness of the opt-out provisions and NPP 2.1(c) generally
- different protection that applies to information used for direct marketing according to the purpose for which it was collected, and whether the inconsistency raises issues for individuals or business
- evidence of the incidence of complaints about the application of 2.1(c)
- business practice in relation to opt-out and whether or not organisations are providing it even when not required to do so and
- how to address issues that arise in relation to privacy and direct marketing for individuals or business.

**What submissions say - the issues**

**Overview**

Most submissions that address this issue focus on whether consumers should be able:

- to opt-in to direct marketing by an organisation, that is, be given the opportunity to elect to receive material, or not, before it is sent or

---

65 See Appendix 6.
66 The number of people in favour of the practice dropped to 29% in a verification survey that followed the main survey.
• to opt-out, that is, that, on receipt of the first (or a subsequent) communication, be given the opportunity to say they do not want to receive further material.

In general terms, consumer organisations favour opt-in and businesses, business organisations and charities favour opt-out.

**Consumers**

In the view of the Consumer Credit Legal Centre (NSW) Inc (62) and the Consumers’ Federation of Australia (65), the direct marketing provisions of the Privacy Act favour the interests of business over those of consumers. The provisions start with the assumption that personal information can be used for direct marketing. Their submissions favour opt-in because it gives consumers some control over the use or disclosure of their personal information.

The Australian Consumers’ Association (15) points out that the corollary of not needing to seek consent (when the personal information has been collected for the purpose of direct marketing, whether directly or from a third party) is that the consumer has no capacity to withdraw consent. It nominates as a useful guide to contemporary thinking the eMarketing Code of Practice67. It also suggests that it would be better to adopt the approach of the Spam Act and to refer to ‘commercial messaging’, which is wider than the traditional direct marketing and avoids boundary issues about what marketing is direct and what is not.

Electronic Frontiers Australia Inc (51) notes that the direct marketing provisions of the Privacy Act are inconsistent with the Spam Act, which requires consent. (The Spam Act on the other hand exempts some senders from the requirement to provide a means of opting out.)

Finally, the Australian Privacy Foundation (90) makes the point that if NPP 2 is working well, then NPP 2.1(c) adds nothing but confusion.

**Business**

Submissions from businesses and business organisations strongly favour opt-out that is, that it is sufficient that organisations give consumers an opportunity to opt-out of any further communication. Compvice Pty Ltd (48), a small business providing voice broadcast services says:

‘Most people do want to receive telemarketing and marketing material. I see this every day. I have developed a simple way for people to opt-out of our voice broadcast campaign pushing the number 9 on their phone. . . We have made 10 000s of calls using this system and found on average less than 5% of people opt-out’.

67 The Code of Practice was registered on 18 March 2005.
It goes on to say that the problem is that there is no simple and effective way for this 5% of people to opt-out of all marketing lists and that there is no ‘Do Not Contact’ list apart from ADMA’s, which is ‘too expensive for some small businesses to access.’

**Opt-out works well for business**

Submissions from business agree that opt-out works well. Suncorp-Metway Ltd (35), for example, provides its customers with an opportunity to opt-out from direct marketing when it collects personal information in the first place. It has had no complaints. ANZ (40) says opt-out is working well – 5% of its customers opt-out. The Australian Bankers Association (70) says there is a low opt-out rate across the industry (less than 10%) and that most customers want direct marketing material.

Coles Myer (60) also says that opt-out is working well. It maintains an opt-out register and regularly washes its direct marketing list against its own register and against the ADMA register. It has more complaints from people not receiving marketing material than it has complaints about junk mail. This is consistent with the experience of Optus (98). It accepts all opt-out requests, has very few complaints and reports that customers want its marketing material.

**Economic considerations**

A number of submissions address the economic implications of changing the law to require opt-in instead of opt-out. Telstra Corporation Ltd (110) says that amending NPP 2.1(c) would result in additional compliance costs that would be unwarranted and not required.

Other submissions look at the broader consequences of change. The Mailing House (79) points out that the direct marketing industry is a major contributor to the economic health of Australia. It says that any change impeding it:

‘would have a serious effect upon the health of this sector and accordingly the financial wellbeing of The Mailing House and the 50 or so families who rely on its financial strength and success to establish and provide their households, educate their children, and provide all the other essentials and luxuries that help make a strong Australian economy’.

Credit Union Services Corporation (CUSCAL) (64) considers the competition implications of any change which, it says, would favour its larger competitors in particular, the major banks.
Charitable organisations

Submissions from several charitable organisations express concern about the possibility of a change to opt-in. The Royal Institute for Deaf and Blind Children (24) says that direct marketing is the most effective way of communicating to the public.

The Cerebral Palsy League of Queensland (44) says that opt-in would result in a loss of income and a loss of employment.

The Fundraising Institute (52) does not support changes to NPP 2.1(c) because, in its view, the provision provides adequate and appropriate opt-out options for individuals.

A participant in one of the stakeholder forums said that to take away the ability of charitable organisations to market directly would impose a significant burden on the community as services provided by charities would be unable to continue.

ADMA submission

In its submission, which is supported by a number of organisations, the Australian Direct Marketing Association (ADMA) (67) states that the most important aspect for an individual when providing personal information to an organisation is to understand how the organisation is going to use it. This is based on ADMA’s own research.

It acknowledges that where an organisation indirectly collects data for the primary purpose of direct marketing the individual may, in some instances, lose control of their personal data. It would support a recommendation that organisations indirectly collecting information for unsolicited direct marketing purposes be obliged to ensure that at the time of collection or as soon as possible after collection (that is, at the first marketing approach) the individual is given an opportunity to opt-out of further direct marketing.

ADMA goes on to say that 80% of respondents to its research are comfortable with organisations collecting and using personal information for direct marketing purposes if, within the first marketing communications and at any time subsequently, they are given an opportunity to opt-out of future communications.

ADMA reports that 68% of respondents to its research would be comfortable with giving organisations their details for direct marketing purposes if they had a right, at any time, to ask the company to stop using it for direct marketing purposes. ADMA says it is standard practice for its member organisations to

---

68 See, for example, Acxiom 71; Opera Australia 104; Australia Post 109.
comply with any request received by an individual not to receive further marketing approaches, even when not required to do so by law.

What submissions say – addressing the issues

General right to opt-out

As discussed above, consumer groups favour opt-in as the general rule and businesses and charities opt-out. In its submission, ADMA states that it would support a recommendation that:

- the individual should have a general right, at any time, to opt-out of future direct marketing approaches and
- the organisation should be obliged to comply with the request within 45 days of receipt.

This is consistent with the Privacy Commissioner's submission to the Senate Legal and Constitutional Legislation Committee Inquiry into the Provisions of the Privacy Amendment (Private Sector) Bill 2000. The submission argued that all organisations using personal information for direct marketing should be required to give the individual the express opportunity at the time of first contact to express a wish not to receive any further direct marketing communications. This could possibly be qualified where the use is within the reasonable expectations of the individual or consistent with the ongoing business relationship of the direct marketer and individual. It would overcome the current distinction in the NPPs between personal information collected for the primary purpose of direct marketing from a third party and personal information and personal information used for the secondary purpose of direct marketing. As long as the process for opting out was not difficult and the request acted on promptly, this would give individuals a degree of control.

On the other hand, the proposal does not go beyond what ADMA says is the current practice. In the view of the Australian Privacy Foundation (APF) (90), a simple across the board requirement to offer an opt-out with every communication is justified by the level of irritation with direct marketing and general lack of awareness and understanding of marketing methods. It goes on to say:

‘This should not be taken as surrendering our position in relation to a positive consent requirement (opt-in) for direct marketing which is outside the reasonable expectations of individuals when their information was collected’.

APF says opt-in should apply to direct marketing which is outside the reasonable expectations of individuals when their information was collected. In addition, the APF supports national 'do not market' registers.
Consent

In the view of Electronic Frontiers Australia Inc (51), a general right to opt-out of future communications is not enough. It says that the NPP2.1(c) exception permitting secondary use of personal information for direct marketing without consent is inconsistent with the recently enacted Spam Act and is totally unacceptable and must be amended. It says personal information should only be used for marketing purposes with explicit consent, not by default.

Other submissions refer to the Spam Act, which requires an individual’s consent to the use of personal information for the purpose of direct marketing. The Australian Communications Authority (94) says that an opt-out regime was found to be unworkable in relation to the sending of commercial electronic messages. The Law Council of Australia (36) recommends that consideration be given to harmonising the direct marketing provisions of the NPPs with the Spam Act.

In Canada, a note to Principle 4.3 of the Personal Information Protection and Electronic Documents Act 2000, dealing with consent, acknowledges that seeking consent may be impractical for a charity or direct marketing firm that wants to buy a mailing list from another organisation. It says that, in such cases, the organisation providing the list would be expected to obtain consent before disclosing personal information.

More effective ‘Do Not Contact’ registers

Some submissions refer to ‘Do Not Contact’ registers. ADMA maintains such a register. Individuals may register their name on a Do Not Contact list in relation to mail, telephone, direct response television, the internet and mobile phones. ADMA members and other organisations can wash their lists against the ADMA list.

However, it is not an absolute and universal ‘Do Not Contact’ list as not all direct marketers are ADMA members, and likewise some businesses may not make the commercial decision to access the names on the list. In addition some small businesses may not be able to afford to use it. Compvice Pty Ltd (48) says there needs to be a cheaper way to access the register.

The Australian Privacy Foundation (90) and Sensis (84) favour ‘Do Not Contact’ registers. In Sensis’ view, the introduction of a national ‘Do Not Contact’ register, could improve privacy protection for individuals.

Inform individuals where information came from

In its submission, ADMA says its experience is that informing individuals of the source of the data being used gives them more control over their personal
information and reduces the number of repeat complaints about unsolicited marketing. It goes on to say:

‘Although ADMA would support a recommendation that NPP 5.2 be amended to require an organisation, on the request from an individual, to inform the individual where the data was sourced, there is a concern that many small organisations, in particular charities, do not currently have the technical capability to comply with such a requirement’.

That being said, ADMA believes the issue is of sufficient importance that organisations should be taking appropriate steps to ensure this requirement can be met. As it is clear that some organisations will need time to make necessary adjustments, ADMA recommends that the requirement to disclose the source of data on request be introduced initially as a best practice guideline with the understanding that, after a period of 18-24 months, the requirement will become mandatory through either a Code rule or legislative amendment.

Few written submissions address this issue. In stakeholder forums, there was considerable support for the idea. In Adelaide, for example, a number of people were in favour of introducing a requirement for direct marketers to tell people from whom they got an individual’s personal information. Participants representing charitable organisations argued that to do so would be too costly and difficult for many charities to implement.

**Options for reform**

**General right to opt-out**

It appears that most organisations give consumers a right to opt-out of future direct marketing approaches whether or not direct marketing is a secondary purpose of collection. This gives consumers a degree of control over the use of their personal information they would not otherwise have. It may not add unduly to compliance costs if organisations are required to give all consumers the right to opt-out of future direct marketing at any time and to comply with the request within a specified timeframe.

**No direct marketing without consent**

A more stringent requirement would be to require direct marketing organisations to acquire the individual’s consent before using his or her personal information for the purpose of direct marketing. The Spam Act provides a precedent for this. On the other hand, requiring consent would increase costs for business and for charities that are dependent on direct marketing to raise funds.
Require organisations to tell individuals where their personal information came from

One of the aspects of unsolicited direct marketing that appears particularly to irritate consumers is that the direct marketer has acquired his or her personal information without the individual’s knowledge or consent. The direct marketer is under no obligation to inform an individual where it acquired the personal information. If it were, the individual could then complain to the organisation that had released the information and, if appropriate, make a formal complaint to the Office. Organisations could be required to tell individuals, on request, the source of their personal information. The organisation would have to tell the individual only where it got the information from, not the original source.

Establish a ‘Do Not Contact’ register

ADMA maintains a ‘Do Not Contact’ register for the use of its members and other organisations. Its existence could be more widely known in the community. Membership of ADMA and the cost of accessing the register on a regular basis may be beyond the resources of some small businesses. A well publicised national register may reduce the level of unwelcome direct marketing. There are precedents in the United States (where 62 million phone numbers were registered in the first year of operation) and the United Kingdom. Different models exist which may exempt certain organisations.

4.4 Recommendations: Direct marketing

23 The Australian Government should consider amending the Privacy Act to provide that consumers have a general right to opt-out of direct marketing approaches at any time. Organisations should be required to comply with the request within a specified time after receiving the request.

24 The Australian Government should consider amending the Privacy Act to require organisations to take reasonable steps, on request, to advise an individual where it acquired the individual’s personal information.

25 The Australian Government should consider exploring options for establishing a national ‘Do Not Contact’ register.
4.5 Awareness of, confidence in and capacity to exercise rights

Law and policy

One of the objects of the private sector provisions is to establish a scheme for the handling of personal information that recognises individuals’ interests in protecting their privacy. The provisions recognise those interests by:

- requiring organisations, where reasonable, to give an individual information about their information handling practices so he or she can make a decision about whether or not to give their personal information
- requiring organisations to get an individual’s consent to collect or disclose in certain circumstances
- giving individuals the right to access information a business holds about them and
- enabling individuals to complain to the Office if a business does not comply with the NPPs.

The provisions aimed to ensure that ‘Australians can be confident that information held about them by private sector organisations will be stored, used and disclosed in a fair and appropriate way’.

Issues

The issues paper suggested a number of topics for submissions related to individuals’ capacity to exercise their right to privacy. It asked about:

- evidence of levels of awareness and the impact of this on the operation of the private sector provisions
- effectiveness of the information provision requirements in raising awareness, how to improve privacy notices and how to improve awareness generally
- evidence of levels of community confidence that privacy rights are protected and ways to encourage confidence, in particular confidence that privacy is protected online and
- information about the extent of individuals’ ability to exercise their rights and how to improve it, and the impact of the Office’s approach to handling complaints.

---

69 Privacy Amendment (Private Sector) Bill 2000 Second Reading Speech, House of Representatives Hansard, 12 April 2000, p 15749. The provisions also apply to non-citizens.
Role of the Office

The Office plays an active role in raising awareness about individuals’ privacy rights and in addressing their concerns about possible interference with their rights. It provides information by way of its information hotline and its web site. The web site contains all the Office’s publications, answers to Frequently Asked Questions, media comments, media releases, speeches, case notes, an online complaint checker, multi-lingual web pages, guidelines, information sheets, brochures and the annual report.

To the extent that the Office’s activities in raising awareness are successful, community confidence that individuals' rights are protected is likely to be increased. If an individual’s privacy rights are interfered with and he or she cannot resolve the issue with the organisation concerned, the Office will investigate the complaint, conciliate it, if appropriate, or make a determination.

Role of organisations

Organisations also play a role in raising awareness and in addressing the concerns of individuals who fear their privacy may have been breached. Organisations collecting personal information are required to take reasonable steps to provide NPP 1.3 or 1.5 notices and must have a privacy policy available to anyone who asks for it (NPP 5). This kind of information may also increase confidence that individuals’ rights are protected. In the event of a breach of privacy, the individual’s first port of call to resolve it is the organisation.

Community awareness survey

Awareness of rights

Community awareness was one of the issues canvassed by the research into community attitudes towards privacy commissioned by the Office in 2001 and 2004. In general terms, it showed levels of awareness were low, although higher in 2004 than in 2001. Only about one in four respondents claimed to know an adequate amount or more about privacy. The number of respondents who were aware that federal privacy laws existed, however, increased from 43% in 2001 to 60% in 2004.

The research showed that 53% of respondents know that government agencies are covered by privacy law; 56% know that banks, insurers and other financial institutions are covered; and 47% that there are some restrictions on charities, private schools and hospitals and other non government organisations.

See Appendix 1.
Confidence rights are protected

The research showed differing levels of confidence that rights are protected depending on the industry. Health service providers have the highest levels of trust (89%), followed by financial organisations (66%), government organisations (64%), charities (54%), retailers (39%), market research organisations (35%), real estate agents (26%) and mail order companies.

Only 9% of respondents trust internet companies, which were intended particularly to benefit from the introduction of the private sector provisions.

Individuals’ ability to exercise their rights

The research showed that 34% of respondents were aware that the Federal Privacy Commissioner existed. (In 2001, 36% were aware.) However, 29% of respondents said they did not know to whom they would report the misuse of their personal information. Of the rest, only 7% mentioned the Federal Privacy Commissioner, the others mentioning a number of different organisations.

Demographic information about complainants

As noted in the issues paper the Office had not previously collected demographic information about complainants. To identify which sections of the community were making privacy complaints to the Office, the Office conducted a three month complainant demographic survey from December 2004 to February 2005.

The Office received a very small response to the survey – 36 responses from over 250 surveys sent. The response rate is too small to rely on as an accurate representation of total complainants, however the Office was able to extract information from its complaint management software that suggests, at least in respect of gender, the survey results may be representational. The figures suggest that it could be the case that the demographic profile of complainants to the Office is not representative of the wider community.

The results of the survey are described in Appendix 13. The Office will continue to collect complainant demographic information.

Multicultural Tasmania (4), while commending the Office on having multilingual pages on its website, recommends the Office think about others ways to distribute privacy information to people from diverse language backgrounds.
What submissions say - issues

Awareness

Most submissions that address this issue believe that community awareness of individuals’ privacy rights is not high. In the view of the Australian Direct Marketing Association (ADMA) (67), community awareness of rights is important and is fundamental to the effective operation of the private sector provisions and the NPPs.

Business SA (92) says there is a widespread lack of understanding of privacy provisions in the community and a significant burden on the private sector to educate the general community about their privacy rights and responsibilities. The Australian Medical Association (29), for example, says that patients still complain to it about possible breaches of privacy.

The Australian Consumers’ Association (15) narrows the issue. It argues that the critical issue is that the consumer is aware of his or her rights when it matters, that is, when he or she has a problem, not at the time of signing up to the service. Lack of awareness goes beyond awareness of consumer rights.

The Australian Compliance Institute (16) says that the obligations imposed on business by privacy laws may undermine consumer expectations. For example, a person may believe he or she is entitled to information about a spouse’s insurance or bank accounts and may not understand why the organisation will not give it to them.

In some areas, however, submissions express a belief that there is a satisfactory level of awareness. The Australian Finance Conference (63) says that in the finance sector, for example, customers are aware of their privacy rights but few exercise them. The Royal District Nursing Service (78) believes its clients are sufficiently aware, except perhaps for its elderly clients. Sensis Pty Ltd (84) believes there is a reasonable level of understanding in the community about its activities.

Participants in stakeholder forums had a lot to say about lack of awareness. One participant, for example, said that people are unaware of their rights and are ‘mystified by multiple jurisdictions.’ Further, they do not understand the differences between policies, procedures and legislation. Another said there must be more awareness raising for the NPPs to work and a better injection of the issues into the culture and that this has to be done by the federal government as the smaller states and territories do not have the money. Some participants asked if the Office was adequately resourced to do what it was supposed to do in raising awareness.

---

71 See, for example, Australian Federation of AIDS Organisations 54; Consumers’ Federation of Australia 65; and Tenants’ Union (ACT) 87.
Confidence

Not many submissions address the issue of community confidence in the protection of rights. The Investment and Financial Services Association (ISFA) (89), a body representing the superannuation, investment management and life insurance industries, states that low level of complaints received by its members, compared to the very large level of transactions, suggests that the community is satisfied with the level of protection provided by its members. The Australian Association of Permanent Building Societies (91) says that public confidence that privacy rights are protected has been substantially increased as a result of the implementation of the private sector provisions.

The Australian Consumers’ Association (15), however, links confidence that an individual’s rights will be protected with the speed and effectiveness of the remedy and expresses concern with the delays and queues that characterise the Office’s complaints handling. Electronic Frontiers Australia (51) goes further in relation to the protection of rights online. Referring to the finding of the Office’s community attitudes survey that individuals trust internet companies less than any other sector, it says that:

‘any attempt . . . to encourage the community to believe that their privacy “rights” are protected online would be highly misleading at best . . . Individuals have almost no privacy “rights” in the online environment and even the few rights they allegedly have are not protected adequately and are difficult, sometimes impossible, to have enforced’.

The submission then goes on to report some collection and disclosure practices of some internet companies. Optus (98), on the other hand, says that the community attitudes survey indicates that a significant proportion of people do not have confidence in companies that do business online, rather than companies that provide internet services.

What submissions say - addressing the issues

Public awareness campaigns

A number of submissions suggest that there should be a campaign to increase awareness about individual privacy rights. Business and consumers alike suggest the Office is the body best placed to conduct public awareness campaigns and that it should be adequately resourced to do so. Acxiom Australia (71) says that what is needed now is a far-reaching education program about rights and responsibilities under the existing law. More specifically, the Salvation Army (74) says that the Commissioner should give special attention to providing information and education and support to social welfare groups.
Telstra (110) suggests the Office should take steps to lift its profile and should offer regular community education about its own role and the steps individuals can take to protect their privacy. On the other hand, Optus (98) suggests the campaign should be targeted to sectors of the community who have not yet become aware of privacy regulations.

In the view of the Australian Compliance Institute (16), the campaign should focus not only on consumer rights but should also educate consumers about business responsibilities. In the context of health, says Australian Federation of AIDS Organisations Inc (54), plain English guides explaining all relevant legislation, not just the Privacy Act, are needed.

**Change privacy notices**

Some submissions link community awareness of rights and improved privacy notices. Australia Post (109), for example, notes that obligations imposed on it and other organisations by NPP 5 have had a positive effect of creating privacy awareness in the community. It suggests that the content, structure and placement of NPP 1.3 notices should be standardised. Privacy notices were discussed earlier in this chapter (4.1).

**Office should improve community confidence**

Submissions generally look to the Office to take action to improve community confidence that rights are protected. The Fundraising Institute (52) suggests a number of things the Office could do, including both promotional and compliance actions. The promotional actions include:

- undertaking strategic marketing to raise community awareness
- authorising the use of a logo indicating commitment on the part of the organisation to good practice and
- encouraging organisations to develop and promote standards of practice.

ADMA (67) says that with its limited resources, the Office needs to develop strategies that seek partnerships with business to encourage community confidence that privacy rights are protected.

The Australian Consumers’ Association (15) says that one of the ways the Office can encourage community confidence that privacy rights are protected is by more vigorous and apparent enforcement action. The Consumers’ Federation of Australia (65) agrees. It also suggests ways in which organisations can encourage community confidence.

**Encouraging individuals to exercise their rights**

The AMA (29) suggests that it would be helpful if the Office kept statistics of complaints against doctors to identify where the medical profession is not complying (to assist in developing education programs for doctors) and where complaints are unfounded (to inform community awareness campaigns).
Resources and educative role

Some submissions explicitly suggest that the Office should be better resourced to fulfil its educative role. ADMA (67), for example, says that the education aspect of the Office’s role needs to be more adequately and suitably funded, and until this is so the effectiveness of the NPPs in protecting personal information will be compromised.

Baycorp Advantage (86) supports an increase in resources to the regulator to support its functions. Finally, the Association of Market Research Organisations and the Australian Market and Social Research Society (61) says that the Office should be resourced to assure the public that the law protects their privacy and that the Office should raise the public’s confidence in what is a good system that is in place to protect their privacy.

Options for reform

Community education and awareness programs could be developed

The scheme established by the private sector provisions of the Privacy Act is complaints based, that is, the Privacy Commissioner primarily acts only in response to a complaint made by an individual. Individuals’ awareness of their privacy rights and how to exercise them, and individuals’ confidence that their rights will be upheld, is critical to the integrity of the scheme. Consumer organisations and business alike acknowledge the importance of community awareness of privacy rights and confidence they are protected. Businesses around Australia have invested considerable resources into ensuring they are privacy compliant and are calling for improved community awareness. The Office could form partnerships with community organisations to develop education programs to raise community awareness about privacy, individual privacy rights and enforcement of rights.

The Office could undertake the program

The functions of the Privacy Commissioner include, among other things:

‘for the purpose of promoting the protection of individual privacy, to undertake educational programs on the Commissioner’s own behalf or in co-operation with other persons or authorities acting on behalf of the Commissioner’72.

The Office of the Privacy Commissioner is best placed to undertake an education program to raise community awareness of privacy and privacy rights. Submissions support this view.

72 Privacy Act section 27(1)(m)
Specifically funded program

The Office would need specific funding to allow it to engage in such a program. Business and consumer organisations have both called for more resources for the Office for this purpose73. The Government could consider funding the Office to undertake a systematic and comprehensive education program to raise community awareness of privacy and privacy rights. This will benefit both consumers and business, which will no longer have to use its resources to explain to consumers why it cannot release personal information.

Office to develop promotional strategies

One way to promote awareness of privacy, and good privacy practice would be to authorise the use of a logo to indicate an organisation’s commitment to good privacy practice. Submissions did not, however, reveal particular interest in it and there is as yet no demand from consumers. Any logo scheme would need to have mechanisms to handle potential breaches of the Privacy Act by logo users. This may have implications for the role of the Office in any logo scheme, particularly in the context of its statutory complaints handling function.

Remove barriers preventing the making of privacy complaints

The complainant demographic survey undertaken by the Office, although somewhat unreliable given the low response rate, suggests that there may be barriers that are preventing certain groups within the community from making privacy complaints to the Office. The Office could take steps to ascertain if there are barriers, for example language barriers, preventing individuals from knowing about and exercising their privacy rights. The Office could then seek to implement initiatives that would remove these barriers.

4.6 Recommendations: Consumer education

26 The Australian Government should consider specifically funding the Office to undertake a systematic and comprehensive education program to raise community awareness of privacy rights and obligations.

27 The Office will continue to collect demographic information about complainants. It will seek to identify and then remove any barriers that prevent sectors of the community from knowing about and exercising their privacy rights.

73 See, for example, Coles Myer Ltd 60; Australian Bankers’ Association 70; Australian Medical Association 29; ANZ 40; Business SA (92); Australian Consumers’ Association 15; Consumers’ Federation of Australia 65.
4.7 Access generally

Law and policy

Introducing the private sector provisions, the then Attorney-General said:

‘It is a fundamental principle of fair information handling that individuals be able to access and correct information about themselves’74.

Subject to specified exceptions, an individual has a right to access personal information an organisation holds about him or her. If one of the exceptions apply, the organisation must, if reasonable, consider using mutually agreed intermediaries. If the individual establishes that the information is not accurate, complete and up-to-date, the organisation must take reasonable steps to correct the information so that it is. An organisation may charge for providing access (but not to lodge a request for access) but the charges must not be excessive (NPP 6).

NPP 6 applies to health information as well as other personal information, supporting ‘what is already good practice among many health professionals’75.

An organisation may withhold access to health information when ‘providing access would pose a serious threat to the life or health of any individual’76.

Issues

The Office receives a number of complaints about failure to provide access, especially in the health area77. The issues paper suggested possible topics for submissions:

- individuals’ experiences in seeking access to personal information an organisation holds about them
- business experiences in giving individuals access to personal information and
- whether measures are needed to address any issues arising for individuals or business in giving or gaining access to personal information.

---

74 Second Reading Speech, Hansard, House of Representatives, 12 April 2000 p 15751.
75 Second Reading Speech, Hansard, House of Representatives, 12 April 2000 p 15751.
76 NPP 6.1(b).
77 Of the 330 NPP complaints against health care providers received by the Office between 21 December 2001 and 31 January 2005, 163 concerned a refusal of access to health records and 19 concerned excessive or inappropriate charges for access (182 in total).
What submissions say - issues

Overview

Most of the submissions that discuss individuals’ access to their personal information are concerned with health information and/or the costs of access either for individuals or for organisations providing it. Some submissions discuss access to personal information in the context of retail, tenancy, insurance and telecommunications.

Health information

Several submissions express concern that giving patients access to their medical records, especially when there are mental health issues involved, may cause harm. The Australian Medical Association Ltd (AMA) (29), for example, supports a person’s right to access information held about them but states that there are occasions when that access can cause harm to the patient or interfere with the therapeutic relationship. The exception in NPP 6.1(b), that providing access would pose a serious threat to the life or health of any individual, sets too high a threshold to overcome the harm that might occur to a doctor-patient relationship or the patient.

Furthermore, says the AMA, NPP 6 does not protect a doctor’s private or preliminary views in the thinking processes required for assessment, diagnosis and formulation of a treatment program. This is of particular concern for psychiatrists who take down facts as described, which may or may not be true, and record their own reactions, which may include an adverse reaction to the patient. In the AMA’s view, it is not appropriate that a patient have access to such notes; even if not life threatening, it can cause disruption to the therapeutic relationship.

Other submissions agree with the AMA’s views. The Mental Health Privacy Coalition (58) would want to ‘white out’ the practitioner’s private thoughts if a patient sought access. Similarly, members of the Australian Psychological Society (103) believe clients may misinterpret what is written.

Life insurance providers have a particular concern. They assess an applicant’s risk on the basis of medical reports but have no knowledge of what the health professional who wrote the report has told the client or whether the client’s life, health or safety might be at risk if they receive the information directly from the insurer78.

On the other hand, the AMA (29) says there is not enough account taken of the need of a carer to know information about the person for whom they are responsible.

---

78 Investment and Financial Services Association Ltd 89.
Finally, a confidential submission says consumers are often confused about access when there is an Advanced Health Directive or a Power of Attorney in place, or when seeking access to the records of a deceased person.

Health information – use of intermediaries

Some submissions state that the obligation in NPP 6.3 to ‘consider’ the use of an intermediary is not strong enough. Privacy Law Consulting Australia (66), for example, says:

‘this principle is effectively meaningless as the requirement to ‘consider’ the use of a mutually agreed intermediary does not place any obligation on an organisation other than to ‘turn its mind’ to providing access through an intermediary’.

Furthermore, the principle does not state what should happen if the parties cannot agree on an intermediary.

Health information – fees

Submissions show a variety of views about the level of fees charged for access to health information.

The Private Health Insurance Ombudsman (10) has received complaints about unreasonable fees charged by a medical practice for access. On the other hand, the Royal District Nursing Service (78) is often left out of pocket when responding to a request for access to information, particularly when the records are no longer on site. In its view the maximum fee allowed under the Victorian Health Records Act is too low. Because the Privacy Act does not include a schedule of fees, a confidential submission says a wide variety of fees are charged giving rise to enquiries from consumers.

Finally, the Australian Physiotherapy Association (APA) (37) says that lawyers often ask for records for use in legal proceedings even though, written for the express purpose of providing treatment, they are unsuitable for use in court. The APA speculates that, as some state legislation caps the amount a practice can charge, ‘some lawyers request records in order to avoid paying reasonable costs for a medico-legal report’. Further, it contends that:

‘some legal firms in Victoria and the ACT are abusing this loop-hole and requesting records under privacy legislation so as to shift expenses to the physiotherapist’.

79 See also Australian Privacy Foundation 90.
Access to other records

The experience of the Tenants' Union (ACT) (87) is that it remains very difficult for private housing tenants to access tenant files held by real estate agents, unlike public housing tenants who can use freedom of information legislation. On the other hand, a large retailer, Coles Myer Ltd (60) has had very few requests for access, fewer than 10 since the Act commenced.

Similarly, member organisations of the Australian Direct Marketing Association (ADMA) (67) have received very few requests for access to personal information. Some submissions, including, for example, Clubs Australia and New Zealand (75) express concern about the costs of providing access. Vodafone Australia Ltd (112) states that it is important to be able to implement cost recovery mechanisms for access to personal information.

What submissions say - addressing the issues

Considering the therapeutic relationship

Submissions suggest a number of ways to address these issues. Some submissions from health care organisations consider circumstances when access should not be given. The Australian Medical Association Ltd (AMA) 29 expresses concern that, in the health care context, there are occasions when access to records could cause harm to the patient or interfere with the therapeutic relationship. The Mental Health Privacy Coalition (58) also suggests that the Privacy Act should be clarified to indicate that the threat of destruction to a therapeutic relationship is a serious risk.

Other aspects of access to medical records

Submissions address other aspects of access to medical records. The AMA (29) says that it is necessary to disclose information about the patient’s ongoing care when he or she is discharged from hospital to the patient’s carer, whether or not the patient consents.

The Investment and Financial Services Association (89) says that insurers want to be able to give information to a patient not directly but via the health professional who supplied the information in the first place, or to the patient’s GP, without having to rely on the NPP 6.1 exception, as is possible under the Health Records and Privacy Information Act 2002 (NSW)

Finally a confidential submission says the Office should issue a fact sheet about access to patients’ health records when there is an Advanced Health Directive or and Enduring Power of Attorney in place.

Use of intermediaries

In the view of Privacy Law Consulting Australia (66), NPP 6.3 which provides for consideration of the use of an intermediary when access is denied should
be removed altogether or else amended to impose obligations on both the organisation and the individual.

Fees for access

As discussed above, a number of submissions consider the fees payable for access to health information. A confidential submission says that the Privacy Act should set a maximum fee for access that is realistic.

The Australian Privacy Foundation (AFP) (90), on the other hand, is happy with the NPP 6.4 provision that charges for access must not be excessive. Its concern is that the Office considers reasonable what the AFP considers manifestly excessive and recommends that the provision is amended to make access free or to set a reasonable cap.

Consumer perspective

The Australian Privacy Foundation (90) makes a number of suggestions for change from the point of view of consumers. These suggestions are:

- NPP 6 should **expressly** require organisations to give access to as much information as possible even when an exception applies to some information.
- An organisation that denies access on the basis of one of the exemptions should be **required** to provide intermediary access (not merely be required to **consider** it). NPP 6 should provide for the Privacy Commissioner to inspect a record on a person’s behalf where access is denied under an exception, and to seek corrections.
- There should be a requirement to consult with third party individuals whose information would be disclosed in response to an access request.
- There should be a prohibition on an organisation requiring an individual to exercise their access rights with a second organisation and then providing the first organisation with the information.
- An individual should not have to ‘establish’ that personal information is not accurate, complete and up-to-date under NPP 6.5; it should be enough for them to have reasonable grounds to believe there is a potential inaccuracy.
- Finally, where personal information is corrected in response to a request under NPP 6.5, there should be an obligation to notify any third parties who are known to have received the information that was not accurate, complete or up-to-date, as exists, ‘where appropriate’ or ‘where practicable’ in legislation in other jurisdictions.
Options for reform

Address concerns about access and the threat to the therapeutic relationship

There are a number of possible ways of addressing these concerns, including further limiting the circumstances in which access might be granted and providing guidance on the existing law. There is no doubt that there are circumstances when access to records may cause a breakdown in a therapeutic relationship and that the breakdown in the therapeutic relationship may constitute a serious risk to the patient's health. However, this does not justify changing the law. Rather, it indicates that there are good reasons for addressing the uncertainties through guidance.

Similarly, the issue of the privacy of the therapist's personal views may be best addressed through guidance. The NPPs allow an organisation to deny access where it would have an unreasonable impact on the privacy of someone else. This could include a therapist's views.

Notify others of corrections made to personal information

When inaccurate information has been passed on to others, it is of little comfort that it has been corrected at source but not elsewhere. When an individual's personal information is corrected in response to a request from the individual, the organisation, where practicable, could be obliged to notify third parties that they have received the inaccurate information.

Use of intermediaries

NPP 6.3 provides that an organisation must, 'if reasonable, consider' the use of an intermediary where it has refused access on the grounds of one of the exceptions to access in NPP 6.1. The right is a very limited one. There is a stronger right to the use of an intermediary under the proposed National Health Privacy Code. An intermediary, a nominated health service provider, may, among other things, consider the validity of the refusal and, if he or she thinks it appropriate to do so, discuss the content of the health information with the individual. The relevant provisions are prescriptive and detailed and are not suitable for inclusion in the NPPs. The NPPs could, however, include a similar right. Alternatively, if the AHMAC code becomes a schedule to the Privacy Act, the matter will be dealt with by that means.

---

80 NPP 6.1(c).
81 This is discussed at section 2.5.
Set fees for access

There is a significant difference in the cost of providing access to records, depending on a number of variables, including whether the records are on site or not, the number of pages involved and the amount of scrutiny necessary. It is not therefore appropriate to set a single fee for access. What may be suitable in one case may be wildly unsuitable in another.

It may be appropriate for the Office to offer some guidance as to what it thinks is appropriate. Alternatively, the Australian Government could introduce a table of recommended fees in a schedule to the Privacy Act. And, if the AHMAC code becomes a schedule to the Privacy Act, the matter may be dealt with by that means.

Office could give guidance re ‘able to establish’ in NPP 6.5

NPP 6.5 requires than an individual ‘establish’ that information is not accurate before the organisation needs to take reasonable steps to correct it. This may be an unduly high standard. It is also unclear. The Office should provide guidance about ‘able to establish’ in NPP 6.5.

4.8 Recommendations: Access generally

28 The Australian Government should consider amending NPP 6 to provide that when an individual’s personal information is corrected in response to a request from the individual, the organisation should be obliged to notify third parties, where practicable, that they have received the inaccurate information.

29 The Australian Government should consider adopting the Australian Health Ministers’ Advisory Council (AHMAC) Code as a schedule to the Privacy Act (see also recommendations 13, 33 and 35). This will address the issue of intermediaries, and the issue of fees for access.

30 The Office will develop further guidance on the operation of NPP 6.1 on ‘serious threat to life or health’, explaining that a serious threat to a therapeutic relationship could be a serious threat to a person’s health. This will go some way towards addressing what appears to be a too narrow interpretation of NPP 6.1(b) by some practitioners.

31 The Office will develop guidance on fees for access to personal information.

32 The Office will develop guidance on the meaning of NPP 6.5 which requires than an individual ‘establish’ that information is not accurate before the organisation need to take reasonable steps to correct it.

82 This is discussed in Chapter 2.
4.9 Transfer of health records to another health service provider

Law and policy

The NPPs do not create specific obligations regarding the transfer of medical records in circumstances where an individual changes from one health service provider to another. In some circumstances, individuals and their providers will simply agree for the records (or copies of them) to be transferred to the new provider. If necessary, an individual may exercise their general access right (under NPP 6) to their health information. If they obtain a copy of their record they can take this to their new provider. However, there is no specific obligation in the Privacy Act requiring a provider to transfer a medical record in full to another provider.

Other regulation may require health providers to do certain things. For example, the Victorian *Health Records Act 2001* requires that if an individual asks, then a health service provider must provide ‘a copy or written summary of the individual’s health information’ to another provider. Furthermore, some professional bodies have noted that in line with good clinical practice and relevant codes of ethics, health service providers should ensure that an individual’s new provider receives adequate information to provide treatment.

What submissions say

This issue did not figure prominently in submissions. However, during consultations it was suggested that while this issue is significant, it may be better addressed at the state and territory level, rather than at the Australian Government level. A reason for taking this approach is that health service providers are registered at the state or territory level, usually by registration boards or similar bodies created under state legislation.

Moreover, the management and handling of patient records generally forms part of a health service providers professional responsibilities for which they are registered. This could be a more appropriate mechanism for setting out, and addressing as necessary, health services providers obligations in this area.

Options for reform

Amend the NPPs - add additional principle

The NPPs could be amended to add a principle (for example, NPP 11) similar to the relevant principles in the Victorian Health Records Act (HPP 10) and draft National Health Privacy Code (NHPP 11).
This principle would state that health service providers would have express obligations to transfer medical records, or copies of them, to a different provider at the request of the individual concerned.

However, this approach introduces a greater degree of prescription to the NPPs than is currently the case. This may not sit comfortably with the high-level, cross-sectoral intent of the NPPs. It should be noted that if the AHMAC code becomes a schedule to the Privacy Act, the matter will be dealt with by that means83.

**No amendment to the Privacy Act - encourage responses by states and territories**

Accepting the view that the transfer of medical records between health service providers is a predominantly professional practice issue, the states and territories (for example, through their medical registration boards) could be asked to set out providers’ obligations in this area.

Jurisdictions could determine whether to set out these obligations in statute or through other professional practice rules and mechanisms connected with provider registration. There would be a need to consider how to ensure national consistency for providers and their obligations across Australia, particularly for those operating (and sharing personal information) across jurisdictions regularly.

**Adopt AHMAC code**

It is anticipated that the draft AHMAC code will be considered by all Australian health ministers in 2005. Following this, the Australian Government could adopt the AHMAC code. If so, the matter will be dealt with by that means.

**No change**

As this was not a high-profile issue in submissions, it may be appropriate to make no regulatory change. Those responsible for health policy across all jurisdictions, as well as the Office, could monitor any emerging issues.

---

83 This is discussed in section 2.5.
4.10 **Recommendations: Transfer of health records**

33 The Australian Government should consider adopting the Australian Health Ministers’ Advisory Council (AHMAC) code as a schedule to the Privacy Act. This will address the issue of the transfer of health records to another health service provider. (See also recommendations 13, 29 and 35.)

34 The Australian Government should consider, if the AHMAC Code is not adopted into the Privacy Act, amending the NPPs to include a new principle along the lines of National Health Privacy Principle 11 in the AHMAC Code.
4.11 Access to health records when health service ceases to operate

Law and policy

When introducing the private sector provisions, the Australian Government recognised that ‘Australians consider their personal health information to be particularly sensitive and that they expect that it will be handled fairly and appropriately by those who come into contact with it.’

One element of fair and appropriate handling of health information is that individuals have a right to access information that a health service provider holds about them. Also, individuals ought to have some control over how their information is handled and by whom.

These choices can be difficult to exercise when a health service provider ceases to operate. Under common law, a provider generally retains ownership of the medical records they create. However, this should not reduce an individual’s right to access their health information should they wish to do so in the context of NPP 6, including the prescribed exceptions to granting access.

Health services ceasing to operate

The Office has become aware of a number of cases where individuals have not been able to gain access to their health information because their health service provider has ceased to operate. For example, a practitioner may have retired, they may have died, or their practice may have closed. Records may be left with other providers, or family members or executors of the previous practitioner, for ‘safe-keeping’. In such cases, an individual’s right of access to their health record can be difficult to guarantee.

In some jurisdictions, specific legislative provision is made for ‘abandoned’ records to be retained by a central body, such as a medical registration board. For example, in Queensland, section 260 of the Medical Practitioners Regulation Act 2001 says the Board may take possession of records it considers abandoned. In NSW, the Medical Practice Regulations 2003 impose obligations on how medical practitioners should handle health records in the event of the disposal of a practice.

---

84 Privacy Amendment (Private Sector) Bill 2000 Second Reading Speech Wednesday 12 April 2000, House of Representatives Hansard p.15750.
In Victoria, the *Health Records Act 2001* through Health Privacy Principle (HPP) 10 sets out obligations for health service providers when they cease to operate. These obligations include advertising the fact of ceasing operations in local newspapers.88

When a health service ceases to operate, this also brings into question a provider’s data security obligations under NPP 4. There is a risk that ‘abandoned’ records may not be afforded adequate levels of storage and security.

**What submissions say**

Similar to the transfer of medical records, this issue did not figure prominently in submissions. During consultations, however, it was suggested that this matter also could be addressed at the state and territory level. Again, a reason for taking this approach is the registration of health service providers at the state or territory level, usually by registration boards or similar bodies created under state legislation.

The Investment and Financial Services Association (89) says that:

‘occasionally, our members encounter the situation where medical records are not available because the GP has retired, died or moved. From an underwriting perspective we would strongly support a national policy whereby an individual’s medical records are retained in a central body when this situation arises’.

The inability for an individual to get access to their medical record because a health service has ceased to operate can affect not only their health care needs, but also their ability to gain other services such as insurance.

**Options for reform**

**Amend the NPPs - add additional principle**

The Privacy Act could be amended in a manner similar to the Victorian HPP 10 and the proposed National Health Privacy Code’s NHPP 10, by adding a similar principle into the NPPs. Such a principle could require providers to do certain things to ensure access arrangements are in place upon the cessation of service, as well as to make individuals aware of how they can seek access to their records.

---

No amendment to the Privacy Act - encourage responses by states and territories

Similar to the approach suggested with the transfer of medical records, it may be reasonable to take the view that the obligations upon providers for handling health records generally is a predominantly professional practice issue. States and territories (for example, through their medical registration boards) could be asked to set out providers’ obligations for securing records upon cessation of a service, and to ensure that access arrangements are maintained.

Jurisdictions could be asked to create central registers for securing and managing ‘abandoned’ records, in a manner similar to that created under the Queensland Medical Registration Board Act.

Adopt AHMAC code

It is anticipated that the draft AHMAC code will be considered by all Australian health ministers in 2005. Following this, the Australian Government could adopt the AHMAC code. If so, the matter will be dealt with by that means.

No change

As this was not a high-profile issue in submissions, it may be appropriate to make no regulatory change. Those responsible for health policy across all jurisdictions, as well as the Office, could monitor any emerging issues.

4.12 Recommendations: Health service ceases to operate

<table>
<thead>
<tr>
<th>Recommendation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>35</td>
<td>The Australian Government should consider adopting the AHMAC code as a schedule to the Privacy Act. This will address the issue of access to health records when a health service ceases to operate. (See also recommendations 13, 29 and 33.)</td>
</tr>
<tr>
<td>36</td>
<td>The Australian Government should consider, if the AHMAC Code is not adopted into the Privacy Act, amending the NPPs to include a new principle along the lines of National Health Privacy Principle 10 in the AHMAC Code.</td>
</tr>
</tbody>
</table>
5 Enforcing individual rights and ensuring compliance

5.1 Introduction

For the private sector provisions to be most effective in protecting individuals’ privacy and in promoting the public interest in privacy, organisations subject to the private sector provisions should be complying with them.

The private sector provisions include a complaints process to enable individuals to complain to the Privacy Commissioner if they believe their privacy has been breached. The Act also gives the Office a power to investigate, on its own initiative, if it thinks an organisation may have breached the private sector provisions.

The scheme does not provide for strict black letter penalties or fines; nor can the Commissioner specify how a particular organisation should comply with the NPPs.

The Office also has a role in providing information and advice to organisations to help them to comply. This issue is discussed in Chapter 6.

5.2 Law and policy

Approach to compliance

The Office takes the approach that compliance will be best achieved by helping organisations to comply rather than seeking out and punishing the few organisations that do not. It assumes that most Australian organisations in the private sector wish to comply with their legal obligations. The Office’s emphasis is therefore on providing advice, assistance and information.

This approach is set out in Information Sheet 13 – The Federal Privacy Commissioner’s Approach to Promoting Compliance with the Privacy Act which is in Appendix 7.

However, the Office actively pursues cases when it identifies breaches of the Privacy Act. It seeks to ensure that organisations remedy breaches and address complainants’ concerns, including by compensating them where that is warranted.

89 In contrast, Part IIA of the Privacy Act which deals with credit reporting includes offences for contravention of a number of provisions, for example section 18K that sets out limits on disclosure of personal information by [private sector] credit reporting agencies.
To date the Office has made limited or no use of the more formal enforcement powers, such as making complaint determinations or seeking injunctions from the court, or publicly ‘naming’ and ‘shaming’\(^{90}\). This is in part due to:

- the Office’s strong focus on conciliation and alternative dispute resolution as a means of resolving individual complaints
- the fact that injunctions are more likely to be relevant in situations where there has been no individual complaint, there is significant and immediate harm and where the respondent is recalcitrant and
- the generally good level of cooperation the Office has received when it pursues issues.

**Complaints process**

**Process**

The complaint handling framework set out in the Privacy Act, and reflected in the Office’s approach, emphasises:

- resolution between the organisation and the individual if possible\(^{91}\) and
- investigation and conciliation where complaints are taken to the Privacy Commissioner or a code adjudicator.

If a complaint cannot be resolved by these processes the Privacy Act gives the Commissioner a range of powers including the power to make determinations.

The Office currently receives approximately 1250 complaints per year. Approximately 66% of these are complaints under the private sector provisions.

Typical outcomes following conciliation include:

- apologies
- access provided and/or records amended
- change in practice or procedure
- staff training and
- monetary or other compensation to redress actual loss or damage.

See Appendix 8 for information about the Commissioner’s powers of investigation and Appendix 9 which includes statistics on how complaints are finalised.

\(^{90}\) The Injunction power may be used by the Office or others. To the Office’s knowledge it has only been used once. See *Seven Network (Operations) Limited v Media Entertainment and Arts Alliance [2004]* FCA 637 (21 May 2004).

\(^{91}\) Privacy Act Section 40(1A).
Where the Commissioner formally determines that an organisation has interfered with the privacy of a person, there are a number of options available to address the issue. The options include:

- making a declaration that the organisation should not repeat or continue the offending conduct
- requiring the performance of any reasonable act or course of conduct to redress the loss or damage suffered by the person concerned and/or
- requiring the payment of a specified amount by way of compensation for any loss or damage suffered by the person concerned.

Loss or damage can include injury to the person's feelings or humiliation suffered by that individual.

If the organisation does not comply with a determination it may be enforced by the Federal Court or Federal Magistrates Court.

Information about complaints

The Office publishes de-identified case notes of some of its finalised complaints that are considered to be of interest to the general public. They illustrate the types of cases resolved by the Office and usually involve a new interpretation of legislation, illustrate systemic issues, or illustrate the application of the law to a particular industry. The case notes do not identify the parties to the complaint. The Office has published 39 case notes since the practice commenced in December 2002.

The Office publishes Commissioner’s determinations in full but suppresses the names of the complainant. It also publishes a variety of complaint statistics and case studies on its website, and in its annual reports.

Powers supporting complaints process

The Privacy Act provides a range of powers and functions to support the complaint handling process and to encourage compliance with the provisions.

These include the power to:

- seek to enforce decisions made by code adjudicators or the Commissioner

---

92 Section 52 of the Privacy Act deals with the Commissioner’s powers to make determinations.
93 An organisation must comply with a determination. If it does not comply the individual or the Privacy Commissioner or a code adjudicator as appropriate may seek to have the determination enforced through the Federal Court or Federal Magistrates Court; the Courts will hear the matter de novo.
94 Section 43(2) of the Privacy Act provides that ‘An investigation under this Division shall be conducted in private but otherwise in such manner as the Commissioner thinks fit’.
Office of the Privacy Commissioner

- make inquiries of third parties
- enter premises (with consent or a search warrant) and
- require the production of information or documents\(^{95}\)
- initiate investigations without a complaint where there may be an interference with privacy (own motion investigations)\(^{96}\).

The Commissioner also has functions to provide advice and to undertake education and awareness programs\(^{97}\).

In addition, the Privacy Act also provides for the Commissioner or others to seek an injunction from the Federal Court or Magistrates Court to stop acts or practices that may be an interference with privacy or to require action to prevent an interference with privacy\(^{98}\).

This enforcement framework is essentially the same as that applying to the Australian public sector since 1989, although with some variations, to reflect the intention that these provisions be 'light touch'. For example, the Privacy Commissioner's power to audit agencies, credit providers, credit reporting agencies and tax file number recipients is not replicated in the private sector provisions. Further, the Commissioner cannot report to Parliament the failure of an organisation to respond to any recommendations following an investigation under section 40(2) of the Privacy Act (own motion investigations).

**Survey of complainants and respondents**

The Office recently surveyed complainants and respondents seeking feedback on the Office's complaint handling process and suggestions for improvements. The Office is now considering the responses and will feed this information into the review of its complaint handling processes. An overview of the survey responses is at Appendix 14. While to some extent responses were coloured by the outcome of the complaint (that is, whether or not it was upheld), many complainants were dissatisfied with the timeliness of the process.

**Review rights**

**Commonwealth Ombudsman**

The Office is subject to review by the Commonwealth Ombudsman with respect to 'a matter of administration'. The Ombudsman often will resolve a complaint through a process of conciliation, but when this is not possible, the

\(^{95}\) See section 43 and section 68 of the Privacy Act.

\(^{96}\) Section 40(2) gives the Commissioner power to investigate a matter that may be an interference with privacy if he or she thinks it desirable without a complaint.

\(^{97}\) See sections 27 and 28 of the Privacy Act.

\(^{98}\) See section 98 of the Privacy Act.
Ombudsman has the capacity, through a report to the concerned agency, to request remedies, for example, where the action:

- appears to be contrary to law
- was unreasonable, unjust, oppressive or improperly discriminatory
- was in accordance with a rule of law but the rule is unreasonable, unjust, oppressive or improperly discriminatory
- was based either wholly or partly on a mistake of law or of fact
- was otherwise, in all the circumstances, wrong or
- in the course of taking the action, a discretionary power had been exercised for an improper purpose or on irrelevant grounds\(^99\).

**Administrative Decisions (Judicial Review) Act 1977**

Complainants and respondents may apply to the Federal Court or the Federal Magistrates Court for a review of ‘administrative decisions’ made about a privacy complaint under the Administrative Decisions (Judicial Review) Act 1977 (ADJR Act). The ADJR Act provides quite a broad right of review. However, it is important to note that the ADJR Act reviews the process followed to make the decision, not the substance of the decision. The Court cannot hear the matter afresh or substitute the decision of the Commissioner with its own. Grounds for a review include a breach of the rules of natural justice, or excess of power, or error of law. If the court finds, for example, that there has been a misuse of power or error of law, the matter will be remitted back to the Commissioner for a reconsideration according to law.

Matters that could be the subject of an ADJR application include:

- a decision that a privacy complaint will not be investigated, or investigated further under section 41(1)(a)-(f)
- a decision not to make a determination under section 52 and
- failure to give to a person who is adversely affected by a decision the reasons for that decision.

**Administrative Appeals Tribunal**

There is no right of appeal to the Administrative Appeals Tribunal (AAT) in respect of determinations about private sector organisations. The Privacy Act does provide a limited right of appeal to the AAT for a merits-based review of the Commissioner’s decisions where the respondent is a federal or ACT agency and only in relation to whether or not to make a determination that a complainant is or is not entitled to compensation\(^100\).

---

99 Section 15(1) of the *Ombudsman Act 1976* sets out the occasions that may give rise to the Ombudsman reporting action to the department or prescribed authority.

100 Division 4 of the Privacy Act.
**Review/enforcement by Federal Court or Federal Magistrates Court**

In addition to the above rights of review, where the Commissioner makes a determination following an investigation of a complaint and the organisation does not comply with the determination, the Commissioner, code adjudicator or complainant, may apply to the Federal Court or Federal Magistrates Courts to have the determination enforced\(^\text{101}\). The courts will hear the matter afresh and apply their own decision.

However, there is no recourse to the courts if the Commissioner does not make a determination or the respondent organisation has complied with a determination (although, as noted above, the ADJR Act is available if the process by which the Commissioner made these decisions is considered unfair or unlawful).

### 5.3 Issues

The issues paper suggested a number of topics for submissions related to enforcement and compliance. These included whether:

- the Office’s overall approach to compliance/enforcement has been appropriate and effective
- the Office’s approach to complaint handling has been sufficiently transparent and accountable
- the Privacy Act provides appropriate rights for individuals as to how their complaint will be handled and the rights of review or appeal available and
- the powers in the Privacy Act are sufficient, in particular to enforce complaint resolutions and/or deal with systemic issues, for example should there be a power to make binding codes, or audit private sector organisations\(^\text{102}\).

### 5.4 What submissions say - issues

**Approach to compliance**

**Support for approach**

Many of the submissions from organisations and business or industry bodies, including Restaurant and Catering Australia (5), Promina (34), Insurance Council of Australia (59), Coles Myer Ltd (60), Australian Bankers’ Association (70) and Optus (98) support the Office’s approach to compliance and argue

---

\(^{101}\) Privacy Act section 55A.

\(^{102}\) By systemic issues we mean issues that are about an organisation’s or industry’s practice rather than about an isolated incident.
that it should continue. These submissions say that the Office’s approach has enabled organisations to implement flexible policies to protect the privacy of individuals without hindering business development. They generally consider that the right balance has been achieved.

In particular Restaurant and Catering Australia (5) commends the Privacy Commissioner’s limited use of formal enforcement powers and its focus on the cooperative resolution of issues. The Insurance Council of Australia (59) also supports the Office’s educative approach to complaint handling.

The Investment and Financial Services Association Ltd (ISFA) (89) suggests that:

‘the effectiveness of the current dispute resolution mechanism has resulted in few judicial decisions on the application and the private sector provisions… [It] strongly supports the continued resolution of complaints by negotiation’.

A number of submissions say that the approach should extend to complaint handling where the focus should emphasise information/advice and conciliation over legalistic determinations103. One confidential business submission thought that existing enforcement powers including in relation to determinations were a ‘powerful enough incentive for organisations to comply’.

**Approach ineffective**

Submissions from the consumer and privacy advocacy groups, including the Consumers’ Federation of Australia (65), the Australian Consumers’ Association (15) Electronic Frontiers Australia (51) and the Australian Privacy Foundation (90) also note the low number of complaints. While the business sector sees this as a positive indicator (see discussion below) these submissions conclude that the educative approach deters individuals from complaining. They say this is because individuals see no strong action or consequences resulting from an organisation’s poor privacy performance.

**Level of compliance**

**Level is about right**

Many submissions from organisations and business groups argue that they or their members have taken significant steps to comply with the Privacy Act. They say that the overall level of compliance is good and the Office’s approach was working well.

---

103 See for example Optus 98, Investment and Financial Services Association Ltd 89, Royal District Nursing Service 78, Chamber of Commerce and Industry of WA (Inc) 77.
A number of these submissions outline the compliance steps they have taken and note the expenditure involved\textsuperscript{104}. These submissions argue for the current approach to be maintained. Some also sought more emphasis on education and/or guidance for consumers and organisations.

Many of these submissions argue that the overall low level of privacy complaints they or their members have experienced is positive evidence of a satisfactory level of privacy compliance. They say this is particularly so taking into account the number of transactions processed. Submissions noting low complaint levels include Coles Myers (60), Optus (98) Sensis 84, ABA (70), Suncorp Metway (35), the Financial Planning Association (85), Australian Association of Permanent Building Societies (91), Australian Finance Conference (63), the ANZ Bank (40) and the Insurance Council of Australia (59). Some submissions put forward statistics supporting this view. For example:

- Suncorp Metway (35) advises that for the period November 2003 to October 2004 it received 9930 complaints of which 149 or 1.5\% were privacy related.
- the Private Health Insurance Ombudsman (PHIO) (10) observes that in 2003/04 it received 3000 complaints of which only 14 complaints were about privacy.
- the Australian Bankers’ Association (70) notes that one of its members ‘reports its analysis of privacy complaints over the past 12 months as representing just .0035% of its total customer base’.
- Credit Union Services Corporation (Australia) Ltd (64) notes that of 347 cases closed by the credit union dispute resolution centre only 9 related to privacy issues.

Coles Myer (60) says that given the low level of complaints it considers the current compliance approach (and powers) to be sufficient.

‘The best protection for a customer…is the organisation’s desire to maintain its reputation and competitive advantage in the market’.

On the other hand the Salvation Army Australia Southern Territory (74) suggests that low levels of complaints can be attributed to lack of awareness of complaints procedure.

**Level may not be adequate**

In contrast, submissions from the consumer and advocacy groups, including those from the Australian Consumers Association (15) and the Consumers Federation of Australia (65) express some strong concerns about the Office’s approach to compliance.

\textsuperscript{104} See for example the Law Council of Australia 36, Insurance Council of Australia 59, Suncorp Metway 35, Coles Myer 60.
It was also a theme in the Office’s public consultations that while many organisations are trying to comply some are not worried about implications of a breach. Some saw this as a possible indication that compliance may not be as widespread and ‘deep’ as it could be. A participant at the Adelaide consultation suggested that if the Office was to ‘out’ poor privacy performance this would then be a point of difference between businesses for consumers to consider; privacy would matter more to business105. Another participant stated that it is difficult to talk some company boards into being privacy compliant when no schedule of penalties attach to the NPPs and commented that ‘if you had audit powers, we might be able to convince our boards to comply’106.

In a similar vein, the Consumers’ Federation of Australia (65) and the Australian Consumers’ Association (15) assert that the Office approach to compliance and the lack of visible enforcement of privacy rights means that organisations are lax about compliance with privacy obligations.

Others support the view that there is no incentive to correct system flaws and that it is easier to simply respond when (the very few) complaints come in rather than comply in a systemic way.107

Comments from some submissions suggest that for smaller businesses, privacy may not be a high priority in the midst of other regulations. For example (83) observes that:

‘All business in Queensland currently negotiates a raft of government (local/state/federal) regulations. For smaller enterprises these regulations are often seen as annoying diversions to the primary purpose of the business: at times they can be very daunting and costly’.

The Australian Chamber of Commerce and Industry (22) makes the similar point (in arguing against the removal of the small business exemption):

‘that privacy compliance costs would be additional to the myriad of other compliance burdens stemming from legislative or regulatory requirements, be they in relation to occupational health and safety, industrial relations or, in particular, taxation’.

In general, the perceived lack of enforcement mechanisms in the Privacy Act especially in relation to determination enforcement is a matter of strong concern amongst the advocacy and consumer groups108.

---

105 Adelaide Stakeholder Consultation 4 November 2004
106 Adelaide Stakeholder Consultation 4 November 2004
107 See for example Consumer Credit Legal Centre 62, Consumers’ Federation Australia 65, the Australian Privacy Foundation 90.
108 See Australian Consumers’ Association 15, Tenant’s Union of Queensland 69, Consumers Federation of Australia 65, Australian Privacy Foundation 90 and Professor Graham Greenleaf 47.
Office does not use existing powers

Submissions, from Professor Graham Greenleaf (47) and some consumer organisations note the very limited use the Office makes of the Commissioner’s power to make determinations. As discussed elsewhere, submissions focus on the perceived lack of procedural fairness and transparency flowing from the lack of determinations.

Professor Graham Greenleaf argues that the limited use of determinations equates to a failure to visibly enforce the law with consequent impact on culture of compliance, compliance risk assessment and so on.

Systemic issues not being addressed

Incidence of systemic issues

Some submissions say that the Office has not paid enough attention to fixing systemic issues, which are causing a large number of complaints. These submissions suggest that the Office needs to consult more regularly with consumer groups to identify systemic issues and to formulate ways of addressing these issues with foresight, instead of merely dealing with complaints once they have arrived at the Office’s door.109

On the other hand a few business submissions are sceptical about the incidence of systemic issues. The Australian Bankers Association (70), in referring to a member banks’ analysis of privacy complaints states that privacy complaints represented 0.0035% of its total customer base and that the complaints had no real pattern, indicating that there were no systemic problems. It states that many of the complaints involved ‘isolated instances of human error’.

Systemic issues and complaints process

A number of submissions are concerned that the Commissioner has limited ability to address broader systemic issues as a result of the Privacy Act’s strong focus upon individual complaints.

The Consumer Credit Legal Centre (62) and the Consumers’ Federation of Australia (65) state that reliance on individual or even representative complaints is ‘inefficient’. The Australian Consumers’ Association (15) raises concerns that the complaints focus disconnects the Office from systemic issues. It argues that the Commissioner should have the power to address systemic problems outside the context of resolving an individual complaint.

The Consumer Credit Legal Centre (62) and the Consumers’ Federation of Australia (65) states there is no incentive to correct systemic flaws:

109 Australian Privacy Foundation 90, Consumer Credit Legal Centre (NSW) Inc 62, Consumers Federation of Australia 65, Australian Consumers Association 15.
‘In most cases, the worst outcome for a respondent is to amend the records. With respect to credit reporting, the cost of dealing with a small number of complaints is apparently less than the cost of ensuring the data is accurate in the first place’.

The Australian Privacy Foundation (90) argues this as well.

While not specifically relating to the NPPs, the Consumer Credit Legal Centre (NSW) (62) raises particular concerns that the Commissioner is not effectively using powers to deal with systemic issues in the credit reporting sector.

The Australian Consumers’ Association (15) argues that over time more enforcement of systemic issues may lower the number of complaints.

More information when systemic issues raised

A number of submissions110 raise concerns about the lack of information provided when systemic issues are raised with the Office. The Consumer Credit Legal Centre states:

‘we are concerned about the lack of information provided to us when we raise issues of what we believe may be a repeated or systemic problem. While our client’s problem may be resolved, we are rarely advised whether there has been any response to what might be a broader problem with a particular credit provider’.

Some also suggest that there is some failure on the part of the Commissioner to recognise the seriousness of broader systemic issues raised by consumer groups and NGOs, accompanied by the suggestion that these groups want closer interaction with the Commissioner.

Not enough powers to ensure compliance

A number of submissions put the view that at present the Privacy Act does not provide sufficient powers to ensure that businesses are aware of their obligations to protect privacy, or know how to implement them in practice and carry through on implementation. They note the lack of audit powers in the private sector provisions and they comment on what they see as a fact that the Office cannot require organisations to comply with ‘own motion investigations’ the Office undertakes111.

110 Consumer Credit Legal Centre 62, Consumers’ Federation of Australia 65 and Australian Privacy Foundation 90.

111 See for example, Australian Consumers Association 15, Consumers’ Federation of Australia 65, Tenants’ Union of Queensland 69, Australian Privacy Foundation 90, Xamax Consultancy Pty Ltd 3.
Ineffectiveness of determinations for compliance and systemic issues

A number of consumer and privacy advocacy groups comment on the effectiveness of determinations in addressing systemic issues in the light of the Commissioner’s determinations in April 2004 following representative complaints about a series of issues arising from the operation of tenancy databases.

The Tenants Union of Victoria (23) claims that evidence suggests the determinations have failed to achieve compliance. It notes that in order to achieve compliance an application must be made to the Federal Court, which is both time and resource intensive.

In addition, it claims that determinations are unlikely to be effective in the awarding of small compensation payments and most importantly, determinations are only applicable to the individual complaint, not to industry wide practice.

Submissions from advocacy groups and representatives\textsuperscript{112} are concerned about the implications of the Privacy Commissioner’s view\textsuperscript{113} that a determination under section 52 cannot require a respondent to do something or refrain from doing something unless the activity relates to matters raised by the complainant.

They are concerned that this view means that the Office cannot address systemic issues raised by a complaint. For example, the Tenants Union of Queensland (69) states that:

‘this can, and has in our view, result in a ‘cat and mouse’ game whereby the respondent makes changes, but not those recommended, but still fails to meet the requirements of the NPPs. Aggrieved parties and their advocates are left to raise new complaints and the process is perpetuated\textsuperscript{114}.’

Professor Graham Greenleaf (47) makes similar points. He notes that respondents are free to ignore recommendations and the only remedy for individuals is to then make a further complaint and that:

‘this could end up in a continuing charade whereby the respondent is told what he cannot do, but cannot be giving binding directions as to what they must do\textsuperscript{115}.’

\textsuperscript{112} Professor Graham Greenleaf 47, Australian Privacy Foundation 90, Tenants Union of Queensland 69.
\textsuperscript{114} Tenants Union of Queensland 69.
\textsuperscript{115} Professor Graham Greenleaf 47.
The overall view from consumer/privacy advocate submissions is that representative complaints, whilst useful in raising systemic issues, were not viewed as being effective in addressing broader systemic issues as the Privacy Act does not provide the Commissioner with a power to enforce systemic remedies.

However, the Investment and Financial Services Association Ltd (89) opposes any proposal to implement systemic remedies as it sees that the current approach is working effectively. Telstra (110) approves of the focus of the NPPs being on interference with the privacy of individuals and submits that the current powers of the Commissioner are sufficient.

**Complaints process**

**Process is not transparent**

Lack of transparency in the complaints process was a major focus of many submissions\textsuperscript{116}.

**People don’t understand the process**

Professor Graham Greenleaf (47), the Consumers’ Federation of Australia (65) and the Australian Privacy Foundation (90) argue that the Office’s complaints process lacks transparency because the Office does not publish a manual which outlines the Office’s policies and procedures when it investigates and resolves complaints. They say that, as a result the parties to complaints can only infer these procedures and policies from the piecemeal information that is publicly available.

**People don’t know what decisions are made or why**

A number of submissions say that people do not know enough about the outcomes of complaints. They say the consequences of this are:

- complainants and respondents do not know how the Office interprets the Privacy Act or what remedies are attainable. Therefore, individuals do not know what arguments to raise or whether their complaint is worth pursuing through the Office
- it is difficult to monitor the adequacy and fairness of the Office’s decisions and remedies; and any mistakes made in the Office’s decision making processes are not exposed

\textsuperscript{116} See for example, Australian Consumers Association 15, Consumers Federation of Australia 65, Australian Privacy Foundation 90 and Professor Graham Greenleaf 47, Electronic Frontiers Australia Inc 51, Consumer Credit Legal Service (NSW) Inc 62 and Professor Graham Greenleaf 47.
legal jurisprudence is not developed in this area of the law and any
deficiencies in the law, which may require law reform, do not become
apparent and therefore do not get addressed.

Professor Graham Greenleaf (47) observes that there is no publicly available
criterion which reflects how the Office selects complaints for publication.

Submissions from privacy advocates and consumers,\textsuperscript{117} observe that the lack of
reported statistics on some aspects of the complaint process means that
the nature of remedies that complainants achieve is not widely known nor is it
possible to assess the Office’s overall performance in complaint handling.
The Fundraising Institute Australia Ltd (52) makes a similar observation.

Some submissions observe that while the published statistics in the
2003-2004 Annual Report show the number of complaints received and
closed and the basis for closing the complaint, there is no indication of the
nature of resolutions achieved.

**Fairness of process**

No review power

Submissions from consumer and advocacy groups, for example, Professor
Graham Greenleaf (47), Consumer Credit Legal Centre (NSW) Inc (62), and
the Australian Privacy Foundation (90) note the lack of a right of review for
complainants or respondents in relation to section 52 determinations made by
the Commissioner.

This issue is set out in detail by Professor Graham Greenleaf (47). The
submission includes the following observations.

‘In my submissions to the Government and to Parliament on the Bill
leading to the private sector provisions I stressed (as did other
commentators) that the lack of any right of appeal against section 52
determinations (to the Federal Court, Federal Magistrates Court, or at
least to the AAT), was extremely unfair to complainants.’

The submission goes on to say that as is noted by the Office’s issues paper,
one of the reasons for this unfairness is that:

‘Respondents have the possibility of having a case heard afresh by
refusing to comply with a determination and waiting for the
Commissioner to seek to have the case enforced in court. However,
this strategy is not available to an aggrieved complainant. Quite apart
from the inherent bias towards respondents in the Act as it stands, it is

\textsuperscript{117} For example, Professor Graham Greenleaf 47, Consumers’ Federation of Australia 65,
Consumer Credit Legal Centre 62, Australian Privacy Foundation 90.
unfair and is unnecessary that there should be no appeal from determinations by the Privacy Commissioner.’

Another common concern in the submissions is the Privacy Act’s lack of a merits-based review process for decisions made under section 41. Submissions say this is particularly a concern, for example, where the Commissioner chooses not to investigate, or investigate further, a complaint on the basis that the Commissioner considers that the respondent has adequately dealt with the complaint, regardless of whether the complainant is satisfied with the respondent’s response.

A few submissions, for example from the Chamber of Commerce and Industry, Western Australia (77) argue that the lack of an appeal right is not unique to the Privacy Act and that it is not clear that it is problematic.

Ending partially complete investigations

Professor Greenleaf (47) submits that there is a lack of procedural fairness in the complaints handling procedure in that the Office may complete partial investigations and then decline to investigate a matter further. In his view procedural fairness can only be ensured if the proper process is in place for the Commissioner to make a formal determination in such cases. Indeed the submission asserts that individuals should be able to insist on the Office making a final determination on a complaint.

**Process is too bureaucratic**

The Consumers' Federation of Australia (65) and Australian Privacy Foundation (90) say that the Office is overly bureaucratic in requiring individuals to first raise the specific issues with the respondent before the Office will handle the complaint.118 The submissions report that, in some cases, this involved writing to the respondent, or respondents several times.119

---

118 Note that section 40(1A) of the Privacy Act says that the Commissioner must not investigate a complaint if the complainant did not complain to the respondent before complaining to the Commissioner. However the Commissioner may decide to investigate the complaint if he or she considers that it was not appropriate for the complainant to complain to the respondent.

119 One submission made this comment in the context of credit reporting for example, where complainants are required to write to Baycorp Advantage in the first instance to obtain a copy of their credit information file and then write to the credit provider about the inaccuracy. While the credit reporting provisions are not under review, this issue is relevant to the NPPs where the credit information relates to commercial credit which is not regulated under the credit reporting provisions.
People are confused about who to complain to

Some submissions from business, government and consumer organisations and from individuals in the health and telecommunications sectors, outlined the difficulties experienced because a complaint could be pursued in a number of forums.

In particular, Telstra (110) notes that its customers could complain to the Telecommunications Industry Ombudsman (TIO) and the Australian Communications Authority or the Privacy Commissioner. In its view the number of possible complaint bodies causes confusion and additional costs. Its preferred view is that the Privacy Commissioner should be the body of last resort and should only get involved after the TIO had considered the matter.

The Department of Health and Ageing (99) put a similar view in relation to complaints in the health sector noting that there was a lack of clarity and definition relating to recourse when consumers feel privacy has been breached. It sought a more consumer friendly approach for dealing with privacy complaints, for example it encourages the Office to develop a Memorandum of Understanding with Health Complaints Commissioners.

However, submissions from regulators with overlapping jurisdiction were more comfortable with the operation of the current arrangements. For example the Australian Competition and Consumer Commission (ACCC) (128) comments that although some complaints may fall within both jurisdictions, this has not been a barrier to resolution. It notes that the Office and the ACCC generally refer complaints to one another and the Memorandum or Understanding has assisted in this.

The Australian Communications Authority (94) says that the lack of clarity about jurisdictional responsibility has not been a barrier to resolution of complaints as parties generally liaise closely and adopted a co-operative approach. However it notes:

‘from a consumer’s point of view, some confusion may arise over which agency a person should make their initial complaint to. Additionally, this lack of jurisdictional clarity has the potential to significantly delay or complicate investigation of complaints and is potentially wasteful of agency resources’.

Delays in handling complaints

A number of submissions questioned the resourcing of the Office to adequately undertake key functions, including complaint handling including ANZ (40), Coles Myer (60), Australian Finance Conference (63), Australian Bankers Association (70), and Baycorp Advantage (86). For example, Coles Myer says:
‘We are aware of consumer advocate criticism of the long delays of matters raised with the Commissioner. We share these concerns. . . . we would recommend the Commissioner be sufficiently resourced to:

- Ensure complaints are allocated in an expedient way and
- To educate individuals that direct contact with the privacy manager at the company involved is the preferred way to resolve an issue.’

Likewise the Australian Finance Conference (63) says:

‘…on the more specific level of complaint handling involving our members individually, there has been concern expressed about the delay in raising the complaint with the member. . . . we recognise that the limitation on the resources of the OFPC may have impacted.’

Other submissions are also concerned about delays in complaint handling.120

A confidential submission from an individual highlights the frustration they felt whilst waiting for their complaint to be investigated. The Australian Consumers’ Association (ACA) (15) notes it is:

‘aware of and concerned by the delays and queues that have characterised complaints handling by the Office over the term of the review. These in turn may well have fed back into a public perception of the Office as being incapable of delivering a satisfactory outcome’. Further, the ACA states a belief that ‘the OFPC has a high rate of discouraged complainants, abandoned complaints and unhappy consumers’.

Tenants’ Union of Queensland (69) says that the ‘resource issue needs to be addressed to allow the Office to discharge its complaint handling function and embed a ‘real respect’ for individual privacy into Australian businesses.’

Respondent organisations are also aware of the problems that have arisen due to the underperformance of the complaint handling function. The ANZ (40) says, that in one case there was a period of 12 months between the time the Office had told an organisation that the complainant had written to the Commissioner and when the complaint was finally forwarded to the respondent.

The ANZ Bank (40) highlighted two problems caused by delay in its submission, in particular:

- delays can have the unintended impact of undermining trust in the regime and lead to calls for a stronger legislative approach, when all that is needed is full use of existing powers and processes and

---

120 For example, Telstra 110, Electronic Frontiers Australia 51 and the Australian Consumers’ Association 15.
• delays can also impact the bank’s relationship with its customer; especially where we are unaware a complaint has been made.

Respondents emphasise that swift resolution of complaints is essential to ensure confidence in the Office and the law.

A number of submissions highlight the fact that prolonged delays in complaint handling reduce the success of complaint resolution and make it difficult to 'mend' the relationship with the complainant\(^{121}\).

### 5.5 What submissions say - addressing issues

#### Transparency

**Publish complaints manual**

A number of submissions, including Professor Graham Greenleaf (47) the Australian Privacy Foundation (90), the Consumers’ Federation of Australia (65) and the Consumer Credit Legal Centre (62) say that in order to cast more light on the way that the Office handles complaints the Office should publish online a comprehensive manual of its complaint resolution policies and procedures, and keep it up-to-date.

**Publish more about complaints outcomes**

Submissions concerned about lack of transparency call for better reporting of the Office’s processes and complaint outcomes in terms of statistical information and more detailed real life examples of closed complaints and how they were resolved.

A number of submissions state that while there has been a marked increase in the number of case notes published on the Office’s website, there is still a need for more examples of real life cases which represent the range of complaints which the Office receives. In addition, these submissions seek detailed information about how complaints are resolved to assist readers to understand the legal issues involved and the Commissioner’s reasoning leading to a resolution\(^{122}\).

Submissions acknowledge that publication of case notes detailing a conciliated outcome may adversely affect the conciliation of a complaint. However they argue this may be overcome by de-identifying complaints or if not possible, considering publication of complaints on a case by case assessment.

\(^{121}\) See for example, ANZ 40, Coles Myer 60, Australian Bankers Association 70.

\(^{122}\) Professor Graham Greenleaf (47), Consumers’ Federation of Australia (65) and Australian Privacy Foundation (90).
To achieve a more systematic approach to the publication of case notes, Professor Graham Greenleaf (47), the Australian Privacy Foundation (90), Consumer Credit Legal Centre (62), the Consumers’ Federation of Australia (65) recommend that the Office adopt a ‘Criteria of Seriousness’ and confirm its adherence to this criteria in the Office’s Annual Report. Professor Greenleaf (47) also recommends that the Office:

- continues to publish statistics on provisions used to dispose of complaints and to publish additional information, such as listing the laws relied upon under section 41(1)(f) and
- publishes statistics of the remedies obtained including the number of cases in which compensation was paid and the amount.

**Greater use of existing powers**

**More proactive**

The Consumer Credit Legal Centre (62) states the Office should be more proactive in addressing systemic issues. The Consumer Credit Legal Centre (62), and the Consumers’ Federation Australia (65) state that reliance on individual or even representative complaints is ‘inefficient’.

**More determinations**

Professor Greenleaf (47) says that there would be more transparency in the complaints process if the Office made greater use of its power to make determinations.

**More own motion investigations**

Many advocacy and consumer groups submit that the Commissioner should make greater use of available powers, including the own motion investigation powers, to address systemic issues. The Australian Privacy Foundation (90) states that:

‘Problems that we see constantly repeated over many years are not being adequately addressed. It should not be necessary to keep bringing individual or even representative complaints, which are a very inefficient way of addressing systemic problems. Instead, the OFPC should be more pro-active in addressing systemic issues using her own-motion investigation powers’.
Fairness

More review

Professor Greenleaf says that both the complainant and the respondent to a privacy complaint should have a right of appeal against any section 52 determinations, in the form of merits review. This could be either to the Federal Court, Federal Magistrates Court, or the Administrative Appeal Tribunal. Other submissions also support this, for example, Consumer Credit Legal Centre (62) Australian Privacy Foundation (90), Professor Graham Greenleaf (47) and the Electronic Frontiers Australia (51).

Right to ask for complaint to go to a determination

Professor Graham Greenleaf (47) argues that if the Commissioner dismisses a complaint under section 41(2)(a) of the Privacy Act on the grounds that the Commissioner is satisfied that the respondent has dealt adequately with the complaint, the complainant should be able to insist that the Commissioner make a determination under section 52 of the Privacy Act. A number of other submissions also support this.123

Professor Greenleaf says that if compensation was involved, this would give the complainant a right to appeal the amount to the Administrative Appeals Tribunal.124 If the respondent was found in breach of the Privacy Act the complainant would have the satisfaction of having the breach publicly acknowledged, even if other remedies were not awarded. He says that the Privacy Act should be amended to clarify that the complainant has this right.

Mixed views about whether the Office should make more use of the determinations power were evident at the Darwin stakeholder forum and included that:

- the fact that few determinations have been issued suggests that no more powers are needed
- more powers are not needed
- the occasional ‘fright’ is needed to keep organisations in line.

123 Consumer Credit Legal Centre 62; Australian Privacy Foundation 90; Professor Graham Greenleaf 47; Electronic Frontiers Australia 51

124 The Office is of the view that currently the Privacy Act does not allow the AAT to hear appeals relating to the private sector.
More help to complainants - streamline process

The Australian Privacy Foundation (90) says there should be an express power for the Office to ‘sort out’ what principles have been breached and who is the appropriate respondent. The submission argues the onus should not be on the complainant as responsibilities for handling personal information can be confusing.

Improving levels of compliance

Powers to enforce own motion investigations

The Australian Consumers’ Association (15) says that the Commissioner should ‘be able to enforce any directions given in relation to findings after an own motion investigation’ which ensures that ‘light handed’ interventions by the Commissioner have the ‘weight of possible further action attached to them’.

Power to audit private sector

The Australian Consumers Association (15), the Consumers’ Federation of Australia (65), Tenants’ Union of Queensland (69), Australian Privacy Foundation (90), and Xamax Consultancy Pty Ltd (3) see an extended audit power as one of a number of necessary strands to a greater level of compliance. Others also argue that an audit power is a necessary response to what they perceive as a current lack of confidence in the community in the Commissioner to protect privacy.

Power to issue binding codes

The Australian Consumers’ Association (15) says that in order to be able to address systemic issues the Office should have the power to issue a standard or binding code.

The Australian Bankers’ Association (70) is opposed to this idea. It states that it ‘would not support the Privacy Commissioner having an “own motion” power to initiate a Privacy Code affecting banks.’ It argues that ‘from the ABA’s perspective the NPPs are working well and this issue is perhaps a matter for other industry sectors to address’.

Other powers to deal with system issues

The Australian Consumers’ Association (15) says that the Office should:
• have the capacity to address systemic privacy problems outside the context of resolving an individual complaint
• be able to find an organisation that breaches privacy provisions
• be able to seek court enforceable undertakings.

Review of resources

A number of submissions\textsuperscript{125} identify that funding to the Office should be reviewed by the government and increased to a level that allows the Office to carry out its functions in an expedient and efficient manner.

The Australian Consumers Association (15) suggests the establishment of a resource stream:

‘to the dispute resolution activities...that is commensurate with and scales to meet the volume of complaints coming to the Office. Preferably this funding would be provided by a scheme whereby organisations complained against bear the cost’.

Are levels of compliance adequate?

Level of compliance

There are grounds for arguing that there is a satisfactory level of compliance with the private sector provisions among organisations. For example, there is evidence that many organisations have taken substantial steps to ensure that they comply. There is also evidence that businesses have made some steps towards compliance. For example, many organisations provide their customers with privacy notices.

Submissions also indicate that they receive very few complaints relative to the number of transactions they process. It may also be argued that the Office receives few complaints considering the number of transactions taking place in the private sector.

The Office accepts these points. In particular it acknowledges that the number of privacy complaints received is very small given the millions of transactions involving personal information each day. It also acknowledges that many organisations are taking significant steps to comply.

\textsuperscript{125} ANZ 40, Business SA 92, Fundraising Institute of Australia Ltd 52, Australian Privacy Foundation 90, Australian Medical Association 29, Baycorp Advantage 86, Consumer’s Federation of Australia 65, Consumer Credit Legal Centre (NSW) Inc 62, Coles Myer 60, Xamax 3, Australian Banker’s Association 70, Australian Finance Conference 63, Australian Consumers Association 15, Graham Greenleaf 47, Tenants Union of Qld Inc 69,
However, it cannot be assumed that as a result of these factors, the level of compliance in the private sector is at an optimum level.

**Complaints as an indicator of compliance**

It may not be appropriate to draw definitive conclusions from the current low level of privacy complaints. There are complex reasons why people do not complain, and low complaint numbers are not necessarily indicative of high levels of compliance. Reasons why individuals may not complain may include:

- individuals are not motivated to complain for a range of reasons including they have not suffered significant loss or damage
- individuals are not aware of the breach
- although the submissions report low complaint numbers the Office is not in a position to know if this applies across the board and, more specifically, how many complaints are made direct to organisations and are resolved at that level
- difficulty in lodging a complaint with the organisation (that is, no privacy contact officer).

Some commentators’ views on this area indicate that most dissatisfied consumers never complain. A United States program, the Technical Assistance Research Program (TARP) has also suggested as many as 95% of dissatisfied customers do not complain to the company concerned.

While companies may assume that a small number of complaints means that consumers are satisfied and that there are no systematic problems, TARP refers to this as the ‘tip of the iceberg’ phenomenon. In addition, according to Hyman et al:

> ‘only a portion of the problems/defects that exist are actually perceived; only a portion of those perceived are voiced; only a portion of those voiced gain access to a complaint-resolving party; and only a portion at each stage are resolved successfully.’

126 Keynote address by Jane Goodman-Delahunt at ASIC’s Stakeholder Forum “Capitalising on Complaints: Insights into Handling Finance Sector Complaints” November 2001


Research shows that while some dissatisfied consumers will voice their complaints to the company concerned, others complain by word of mouth to friends, family members, neighbours and their community. Others, instead of complaining, will simply change providers. In that case, it could be argued that the provisions and ‘the market’ are working.

Factors such as the effort required to confront the organisation and to articulate the problems as well as anxiety over what may happen when the organisation is confronted have been raised as reasons why individuals would not make a formal complaint to management.

**Compliance may be uneven**

It is clear that the banking and insurance sectors have paid considerable attention to privacy compliance. However, there is anecdotal evidence from other submissions, the consultations and the Office’s own experience that suggests that the depth of privacy compliance is not uniform and that some organisations may not be following up initial compliance efforts or may not have implemented privacy requirements at all. The Office notes here the comments in some submissions about the overall compliance environment. These include the lack of incentive in the Privacy Act and the Office’s approach to compliance for many organisations to implement privacy in a systemic way and the complexity of the regulating environment in general.

As some submissions pointed out earlier, smaller businesses often see the raft of government, local and federal regulations, including occupational health and safety and particularly taxation, as annoying, costly and expensive diversions to the primary purpose of business. Complying with privacy requirements, particularly if regarded as a low risk issue, is likely to be a lower priority than such matters as taxation or other more immediate regulatory concerns.

**Monitoring compliance**

The Office has limited ability to objectively assess current levels of compliance. This is in part because the Commissioner’s monitoring powers are limited. The Office does not have the power to do random checks on organisations to see if they are complying. The currently available investigative options are the own motion power, which can be triggered where there may be an interference with privacy and the Commissioner considers it

---

130 Hyman et al suggest as many as 54 percent complain to someone else.
133 See for example, Commerce Queensland 83, Australian Chamber of Commerce and Industry 22.
desirable to investigate, or by undertaking an audit by invitation\textsuperscript{134}. The Office could also rely on its educative functions to seek information via surveys, consultations and the like.

Also, in line with the ‘light touch’ approach of the private sector provisions, organisations do not have any obligation to report to the Office on their compliance.

\textbf{Is change needed?}

Concerns raised in submissions and from the Office’s own experience suggest that there is room for improving compliance and its complaints process. This can be done in a way that increases the incentive for businesses to comply while having little impact on organisations that are actively and fully complying. These could include greater guidance and education and awareness programs and improving existing processes, as well as strengthening enforcement powers.

\textbf{Enforcement powers}

The House of Representatives Standing Committee on Legal and Constitutional Affairs\textsuperscript{135} noted without making a formal recommendation, that there appeared to be some limits to the enforcement regime in the Privacy Act.

This is supported by the Office’s experience that more directive powers may be desirable particularly where systemic issues arise, either in the course of a complaint, or in the context of an own motion investigation.

The Office’s experience also indicates that while a vast majority of organisations comply with the Offices directions when it finds a breach, there are some that do not. Although this occurs in few cases, the failure to comply devalues the privacy scheme and reduces the incentives for others to comply and also means that organisations that do comply do not receive the full benefit of their conscientious behaviour in terms of level playing fields. Apparent lack of enforcement also discourages individuals from complaining.

\textbf{A more active and transparent approach}

The benefits that are likely to flow from a more transparent and active approach to compliance could include:

\textsuperscript{134} Section 40(2) and section 27(3). No organisation has asked the Office to carry out an audit on it.

increase in public confidence in the Privacy Act because serious issues or recalcitrant organisations are seen to be dealt with
businesses making serious efforts to comply would not be disadvantaged, that is the playing field would be more level
there would be more published information about how the Office applies the Privacy Act.

**Systemic issues**

The Office has a strong focus on individual complaints although it does also respond to systemic issues raised in complaints or identified by other means to the extent possible. The focus on individual complaints is in part because complaint investigation is a non-discretionary function.\(^{136}\)

There is some evidence that the Office’s limited focus on systemic issues and its lack of power to deal with systemic issues is out of step with best practice for complaint handlers. For example Louise Sylvan (then of the Australian Consumers' Association) in representing to the 2003 National Dispute Resolution Advisory Council Conference\(^{137}\) in identifying good practice in complaint handling noted that:

> ‘A scheme must be underpinned by a comprehensive and efficient complaints handling mechanism. Systemic analysis is required which seeks to eliminate systemic recurrence of issues and to achieve resolution with finality….. the addressing of systemic issues to preventing recurrence, and public reporting (or name and shame)’.

A greater focus on analysing complaints, following up leads, conducting more own motion investigations to identify systemic issues and so on could also feed into education and guidance activities.

The Office has had some notable successes in encouraging organisations to make systemic changes to systems and practices\(^{138}\). However, the Office has experienced difficulties in dealing with systemic issues in particular cases. For example there have been a number of cases involving the handling of old medical records both in terms of security and in ensuring that individuals can continue to access their records.

---

\(^{136}\) Section 40(1) provides that the Commissioners ‘shall’ investigate a complaint if the act or practice may be an interference with privacy.

\(^{137}\) ADR: A better way to do business

\(^{138}\) Examples include: a credit provider’s mass removal of all payment defaults from a consumer credit reporting agency; significant system changes to information handling systems by a information technology company; and systemic information collection practices by a member of the finance industry.
The Office has also encountered difficulty in dealing with privacy issues arising from the operation of tenancy databases. For example, the Commissioner cannot require tenancy database operators to take a particular set of compliance actions either in the course of a determination or following an own motion investigation.

5.6 Options for reform

More education and awareness

As outlined in Chapters 4 and 6 of this report, there is considerable room for greater education and awareness among organisations and consumers. Better informed consumers are likely to ask that organisations comply with their obligations. Also, if consumers demand this, businesses are more likely to see the business advantage in practicing good privacy. Also, it may be that some smaller organisations are still unaware of their need to comply with the private sector provisions, or even if aware, unsure how to go about complying. The recommendations in Chapter 4 and 6 relating to a new consumer and business awareness program are likely to have some impact on the level of business compliance.

Increase transparency in complaints process

Publishing more information

Good reasons for publishing more information

The submissions seeking greater transparency made a number of suggestions for reform. In general, the objective of greater transparency, short of routinely naming both parties, in complaint handling processes and outcomes, is likely to benefit both complainants and respondents. Individuals and organisations will be negotiating with greater knowledge of likely outcomes. Organisations and their advisors will have more detailed information about how to comply. The Office’s decisions would be more open to scrutiny. However, it does not appear to be common practice for regulators to publish manuals which set out in great detail their complaints processes.

Publishing Outcomes of Conciliation/Complaints in other jurisdictions

Many complaints bodies publish de-identified case notes or similar. However these vary in length and number. Australian complaint-handling bodies that publish a select number of de-identified case notes include Office of the Victorian Privacy Commissioner, the Anti-Discrimination Commission Queensland. The Office of the New South Wales Privacy Commissioner does not publish any case notes or report on conciliated complaints. The full texts
of cases that have gone through the New South Wales Administrative Decisions Tribunal are publicly available.

Decisions made by the Human Rights and Equal Opportunity Commission (HREOC) between 1985 and 1999 are available on the Australian Legal Information Institute website. From 2000, the public hearing and determination process was passed to the Federal Court of Australia. These decisions are available online through the Federal Court of Australia’s website and the Federal Magistrates Service website. HREOC also maintains a de-identified register on its website of all conciliated cases. The complaint summaries in this register provide information about the terms of settlement including the amount of compensation awarded, if any.

The New Zealand Privacy Commission and the Office of the Privacy Commissioner for Personal Data, Hong Kong publish a number of de-identified case notes on their websites. The Office of the Privacy Commissioner of Canada publishes de-identified case notes for both settled and early resolution cases. The Canadian Commissioner has also published an incident summary. This is a summary of a case which is not the subject of a complaint but has been brought to the attention of the Commissioner (similar to an own-motion investigation under the Privacy Act).

It would appear from this survey that publishing more information would bring the Office more closely into line with other complaints handling agencies. However, it does not appear to be common practice to publish in a way that includes identified information.

The Office could maintain a de-identified register of the outcomes of all the complaints it conciliates. It could provide more information about the outcome of all complaints or it could continue to produce case notes.

**Review use of determination power**

Making more determinations would address a number of concerns about the transparency and fairness of the current approach to complaint handling. It could particularly address concerns expressed about situations where the complaint does not seem amenable to resolution by conciliation or where there is a public interest in proceeding to a determination. This approach could also provide a solution to the expressed concern of some consumers and advocates that the enforcement of the Privacy Act is ‘soft’.

In addition to promoting confidence for consumers, there would be clear benefits for organisation in terms of certainty. There would be more published decisions on how the Privacy Act applies.

---

The possibility of finalising more complaints by determination could have resource implications for organisations and the Office. Determinations, particularly where they involve oral hearing are potentially more costly for the Office to administer. The Office could focus more directly on monitoring compliance with determinations and if organisations do not comply, in seeking enforcement through the Courts.

More external review

Providing additional appeal rights may create a fairer process for individual complainants in areas where currently there is no review. It could create greater transparency and scrutiny for the Office’s decisions on the private sector provisions. Although industry based complaint handlers do not have review rights, the lack of merits review for the Office’s key decisions, particularly determinations, appears to be out of step with other government based authorities.

For example, the Privacy Act, when compared to other statutes providing for a right of complaint, is unusual both in terms of containing a power to make final determinations about a complaint and in providing limited avenues of appeal to judicial decision. Appendix 12 sets out the position in relation to a number of similar statutes. The role of positions similar to the Commissioner’s is more often to attempt to resolve a complaint by conciliation. Where conciliation fails or is not possible the more usual process is a court hearing with accompanying rights of appeal.

On the other hand, it might be said that creating appeal rights might result in a more legalistic and burdensome process which is not consistent with a ‘light touch’ scheme. It could be argued that rights of appeal that do exist have not been very much used, and so creating additional ones is unnecessary. Also, the Commissioner is in effect a body of appeal (from decisions made by the organisation) and that it would be unnecessary to provide additional levels of appeal, particularly given that the process the Commissioner uses is separately subject to ADJR Act review. In this regard it is worth noting that the Parliament provided for determinations by code adjudicators to be reviewable by the Commissioner.\(^{140}\)

The question of appeal rights was considered by the House of Representatives Standing Committee on Legal and Constitutional Affairs which inquired into the Privacy Amendment (Private Sector) Bill 2000\(^{141}\). The Committee mentioned a number of issues, including concerns about perceived lack of appeal rights in respect of the enforcement regime in the Privacy Act. It also noted that some witnesses expressed concerns about the appeal framework as framed in the Bill, including higher compliance costs for business compared to an industry scheme with no appeal rights and the

---

140 Section 18BI  
threat of judicial review would make complaint handling bodies more formal and legalistic.

The Committee noted both set of concerns. While its report did not make a recommendation, and consequently the Government response to the report did not consider the issue, it did note that the enforcement and appeal provisions in the Bill appeared to need further attention142.

As discussed in this report, the Commissioner is reviewing the Office’s complaint handling process, including the circumstances in which complaints will be finalised by determination. These circumstances could include where the complainant and respondent cannot agree on a resolution by conciliation. This change in approach, which would not require changes to the Privacy Act, and may meet one stream of concern in the submissions about lack of review rights.

**Fairer process**

Some submissions identify areas where the Office’s complaint handling processes seem overly bureaucratic, for example where the complainant has not identified the correct respondent and is told they need to take this step before the Office will respond.

There would be clear value in looking at the process to ensure that it meets external standards for complaint handling and alternative dispute resolution (ADR) and to make it more user friendly for both parties where the law and resources allow.

**Make better use of existing powers**

**Greater use of own motion powers**

**Existing practice**

The Office undertakes own motion investigations in a range of circumstances. Typically, the Office becomes aware of these matters through reports by individuals, or the organisation concerned or through the media. In some cases, the Office also follows up matters that have been identified through complaints.

---

142 ibid page 126
The table below shows the total number of own motion investigations logged on the Office’s complaint handling system over the past five years. Not all incidents logged are investigated. The Office applies risk management criteria that include, the seriousness of the incident and the number of people affected (see Appendix 10 for more details about the Office’s use of the own motion power).

Table: Number of own motion investigations and complaints registered

<table>
<thead>
<tr>
<th>Time period</th>
<th>No of OMIs</th>
<th>Complaints (not including OMIs)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 July 2000 – 30 June 2001</td>
<td>10</td>
<td>194</td>
</tr>
<tr>
<td>1 July 2001 – 30 June 2002</td>
<td>48</td>
<td>611</td>
</tr>
<tr>
<td>1 July 2002 – 30 June 2003</td>
<td>64</td>
<td>1090</td>
</tr>
<tr>
<td>1 July 2003 – 30 June 2004</td>
<td>69</td>
<td>1276</td>
</tr>
<tr>
<td>1 July 2004 – 1 Feb 2005</td>
<td>59</td>
<td>724</td>
</tr>
</tbody>
</table>

**Value in more own motion investigations**

Undertaking more own motion investigations would be a practical way of addressing systemic issues independently of complaints. However, doing this would have an impact on the Office’s resources. In addition, for the investigations to be of greater benefit, the Office would need to have the power to direct organisations to address any issues found and then to enforce those directions.

It may be that if the Office carried out more own motion investigations with enforceable directions, this would be sufficient to enable it to address systemic issues.

**Power to enforce own motion investigations**

Problems caused by lack of enforcement power

The Office has experienced some difficulties in dealing with potential privacy breaches where there is no individual complainant and where the respondent is not cooperative or where there is a need to respond quickly to systemic poor privacy practices, for example in relation to tenancy databases. In this respect it would appear that the Office’s powers may be out of step with other similar regulators.

Other regulatory regimes

A number of similar regulatory regimes include more directive enforcement powers. For example, under section 48 of the *Information Privacy Act 2000* (Vic), an organisation must comply with a compliance notice served on it.

---

143 Section 40(2).
Under Section 44(1) of the *Information Privacy Act 2000* (Vic), the Victorian Privacy Commissioner may serve a compliance notice on an organisation if the organisation has done an act or engaged in a practice in contravention of an IPP or applicable code of practice and the act or practice:

- constitutes a serious or flagrant contravention or
- is of a kind that has been done or engaged in by the organisation on at least 5 separate occasions within the previous 2 years.

Section 44(5) enables the Victorian Privacy Commissioner to act on his or her own initiative. It is an offence under section 48 not to comply with a compliance notice. Section 66(1) of the *Health Records Act 2001* (Vic) enables the Health Services Commissioner to serve a compliance notice on an organisation in the same way as the Information Privacy Act 2000. Section 66(5) enables the Health Services Commissioner to act on his or her initiative. Failure to comply with a compliance notice is an offence under section 71 of the Health Records Act 2001 (Vic).

Under the *Trade Practices Act 1974*, the Australian Competition and Consumer Commission (ACCC) has the power to accept court-enforceable undertakings\(^{144}\). It may use this power to resolve a possible contravention of the Act by deciding to accept formal administrative settlements or undertakings from businesses, including in addition to or in lieu of taking legal proceedings. The ACCC advises that it does not accept offers of such undertakings unless the undertakings are to be made public and do not contain denial of contravention of the Act. The ACCC may enforce such undertakings in court if they are not honoured.

Under Section 155(2) of the *Anti-Discrimination Act 1991* (Qld), the Queensland Commissioner may initiate an investigation if

- (a) during the course of carrying out the commission's functions, a possible case of a contravention of the Act against a group or class of people is discovered, the matter is of public concern and the Minister agrees; or
- (b) an allegation is made that an offence against the Act has been committed; or
- (c) during the course of carrying out the commission's functions, a possible offence against the Act is discovered.

Under Subsection 155(4), if the Queensland Commissioner investigates under subsection 155(2) and the matter cannot be resolved by conciliation, the Queensland Commissioner may refer the matter to the tribunal as if it were a complaint. In such an instance, the Queensland Commissioner acts as if they were the complainant (section 155(5)).

\(^{144}\) See Section 87B of the *Trade Practices Act 1974*.  

---

The Review of the Private Sector Provisions of the Privacy Act 1988

156
Power to audit private sector

Existing power

In general, the Commissioner does not have an audit power in relation to the private sector provisions\(^\text{145}\). The Commissioner can audit an organisation if invited by the organisation to do so, however, to date there have been no audits under this function\(^\text{146}\).

Benefits of audit power for private sector

Having a private sector audit power may increase community confidence in the efficacy of the Privacy Act and give the Office an additional power to identify systemic issues and to monitor responses.

However, if the Office were to have the power to audit the private sector, this would have resource implications. It currently carries out limited audits in those areas in which it has the power. In addition, it could be argued that this is a role that a number of private sector consultancy firms carry out, and should not be one taken on by the Office.

A more appropriate role may be for the Office to provide information on the value of auditing to organisations as evidence of compliance in the event of complaints. The Office could also develop and provide privacy audit training for organisations. Another option could be for the Office to provide privacy audit resources including auditors who have privacy expertise. In the latter case the Office could consider whether some form of privacy auditor accreditation would be useful or necessary.

Other power to address systemic problems in complaints

Extend section 52 powers

The Privacy Act could be amended to extend the Commissioner’s powers under section 52 to apply specific systemic remedies to individual and representative complaints. This would enable the Commissioner to prescribe a specific course of action to eliminate acts and practices in a systemic way as part if its complaints system. This would be an efficient and effective way of addressing systemic issues that it comes across in the course of handling complaints. This is important as complaints are the main way that the Office becomes aware of privacy practices.

\(^{145}\) There is an audit power associated with the tax file number and credit reporting provisions see sections 28 and 28A.

\(^{146}\) Section 27(3) of the Privacy Act.
Power to issue binding guidelines

The Privacy Act could be amended to give the Commissioner the power to issue binding guidelines. This could be a useful tool in contexts where the Office becomes aware of systemic issues and wishes to issue general, but binding guidance to ensure that all organisations comply with them. This creates a more level playing field among organisations, and ensures that conscientious organisations are not commercially disadvantaged.

Such guidelines could address aspects of the NPPs as they are applied in specific contexts, for example, steps to be taken in a particular industry sector to ensure personal information is accurate, complete and up to date. They could overcome uncertainty in application of NPPs in particular situations. It would also benefit consumers to have a more specific idea of their rights.

Binding guidelines would be developed following consultation with affected stakeholders and may need to be disallowable instruments. The Commissioner could also take into account any potential negative impact in deciding whether to issue binding guidelines. Factors to consider here could include whether binding guidelines would add to the complexity of the privacy regime and whether this was warranted in the circumstances.

Power to issue binding codes

An alternative or addition to the options discussed above could be a power under the Act to be able to issue a binding code. Various options for this are discussed in Chapter 2. This may be the best solution in a narrow range of cases such as, for example, the operation of tenancy databases. While, in general, it is preferable and appropriate that the organisations are able to make their own judgments about the steps needed to comply with the NPPs, it may not be the best outcome for some sectors.

The possible value in a mechanism such as a binding code can be illustrated by looking at issues that were considered in the four determinations made in 2004 following representative complaints about a tenancy database operator and in the general context for these complaints. The determinations considered questions such as:

- whether the charges for providing access were excessive – NPP 6.4
- what steps are reasonable to ensure personal information is ‘accurate, complete and up-to-date’ – NPP 3
- the nature and timing of notice to individuals that they may be listed with a tenancy database and
- the length of time a tenancy default listing could be retained on a tenancy database.

The Commissioner found breaches on a number of these issues and made a number of recommendations to prevent the problem reoccurring in the future. However, the Commissioner stated, for example, in Determination No. 2 of 2004 that:

‘The complainants have asked me to make a declaration requiring TICA to develop new forms to meet its obligations under NPP 1.5. I am not satisfied that I should do so. While I have declared that TICA should not repeat or continue conduct which constitutes an interference with the privacy of an individual, I do not, in my view, have the power under section 52(1)(b)(i)(B) to otherwise generally prescribe how TICA should act.’

In practice, the impact of the Commissioner’s determinations on the tenancy industry appears to have been limited. The Office continues to receive complaints from individuals; about tenancy database operators and that these complaints raise many of the same issues that were dealt with in the determinations as well as new issues.

A number of database operators have called for the Commissioner to ‘rule’ on a number of aspects of the NPPs, including for example, the timeframe for keeping listings and fees for access. The interest here seems to be in seeking certainty and to some extent a level playing field.

A binding code could set specific direction in relation to the accurate content of listings (NPP 3) or time limits for removal of listings from a tenancy database (NPP 2.1 and NPP 4.2). It could also address matters such as appropriate mechanisms for dispute resolution.

**Improve liaison with overlapping complaint handlers**

The Office could liaise closely with these bodies to ensure that privacy complaints are handled efficiently and to minimise confusion and costs for both individuals and organisations. It could have a memorandum of understanding to ensure that the most appropriate regulator is considering each complaint and to improve overall complaint-handling.

Care would be needed to ensure that any memorandum of understanding did not limit individual’s rights under the Privacy Act. However, this is a matter that could be addressed, for example, by agreement that bodies would provide information about rights under the Privacy Act in their publications. That said, where individuals come to the Privacy Commissioner after their complaint has been considered by another body, the Office’s approach generally would be to take account of investigations by other bodies in deciding whether it should investigate a matter and has done so in a number of cases.
The Office has had discussions with other bodies that handle privacy or privacy related complaints, including the Telecommunications Industry Ombudsman and the Banking and Financial Services Ombudsman. There is a common interest in ensuring that as far as possible a complaint is handled by the appropriate body. This avoids the complaint ‘merry-go-round’ and ‘double-dipping’ (where consumers approach consecutive bodies seeking a better outcome).

**Advice about complaint rights**

Many organisations already tell people in their privacy notices about how to complain to the organisation and also the Office. However, the NPPs do not currently require this.

This change could complement other measures to ensure individuals are aware of their rights and how to pursue them.

A partial model is found in paragraph 3.7 of the Credit Reporting Code of Conduct that requires credit reporting agencies to immediately inform individuals that they have recourse to the Privacy Commissioner, if the credit reporting agency establishes that it is unable to resolve the dispute.

This could be a useful tool in the overall strategy to raise awareness and identify and remedy systemic issues. It could be achieved by amending the NPPs or by the Office issuing an information sheet or other guidance.

**Address delay in handling complaints**

The issues paper highlighted that individuals who complain to the Office generally face a considerable delay (currently between 10 and 12 months) before the Office can handle their complaint. This is primarily due to the volume of complaints the Office has received since the private sector provisions came into effect.

The Office has given priority to its complaint handling function so as to minimise delay in complaint investigations for complainants and respondents. It has diverted resources from other areas of responsibility including auditing of Commonwealth agencies, towards complaint handling on the rationale that increasing complaint backlogs had the potential to undermine the operation of the Privacy Act.

Submissions from all quarters express dissatisfaction with the length of time it currently takes the Office to handle complaints. It complicates business relationships and consumers want outcomes.
Review practices

The Office is keen to ensure that complaints are dealt with in a timely manner and that the parties are not disadvantaged by any delay. To this end since 2001 the Office has reviewed and modified its practices by employing a number of strategies to deal with the complaint numbers. These include:

- introducing a new complaints management system
- implementing a more rigorous system to triage complaints received
- improving workload management
- more standardisation of correspondence
- a system for referring certain queued complaints back to the respondent and
- employing a web based tool that allows potential complainants to test if the Commissioner is likely to be able to investigate their complaint.

The following statistics give a brief overview of the extent of total complaints and enquiries to the Commissioner.\(^{148}\)

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Enquiries to Hotline</td>
<td>8177</td>
<td>21033</td>
<td>21290</td>
<td>20208</td>
<td>13541</td>
</tr>
<tr>
<td>Written Enquiries</td>
<td>884</td>
<td>2700</td>
<td>2382</td>
<td>2206</td>
<td>1301</td>
</tr>
<tr>
<td>Complaints under section 36</td>
<td>194</td>
<td>632</td>
<td>1090</td>
<td>1276</td>
<td>839</td>
</tr>
</tbody>
</table>

The Office is concerned the complaint resolution process is impaired if complainants wait a long period before their matter is investigated. As time passes the quality of evidence deteriorates. The Office is also concerned that the delay may allow poor privacy practices to continue unchecked and that systemic problems are undiscovered.

Further review complaints practices

The Office could consider further streamlining its processes but it would need to consider the extent to which it could do so without undermining principles of natural justice.

\(^{148}\) The Commissioner’s annual reports, available from the website at http://www.privacy.gov.au/publications/index.html, include these and other statistics about complaints and enquiries. Section 4.3.1 of the Commissioner’s annual report 2000-2001 notes that 35% of these calls were outside the Act’s jurisdiction.
Cost recovery

The Office could consider charging respondents to handle complaints about them. It could also consider charging complainants. However, the Office notes that it is not aware that other complaints handlers apart from Courts charge applicants to handle disputes.

Power to decline to investigate and other strategies

Other options for responding to the delay could include giving the Commissioner stronger powers to decline to investigate complaints where there appears to be little public interest (for example, where there is minimal apparent harm, or the matter has been considered before and the organisation has changed practice).

As discussed above, the Office could give greater emphasis to complaints or investigation into systemic issues with a view to preventing future harm (and privacy complaints). However, in the short term the latter strategy may mean that the backlog of individual complaints gets larger.

5.7 Recommendations: Complaints handling and compliance

Approach to compliance

37 The Office will maintain its current approach to compliance including the focus on attempting to conciliate complaints in the first instance as set out in Information Sheet 13. However, the Office will consider whether it might be appropriate in some circumstances to use its other powers earlier, such as the determination making power.

38 The Office will consider options for providing more feedback on systemic issues either in advice or guidance or in some form of regular update to stakeholders.

39 The Office will consider promoting privacy audits by private sector organisations, including by providing information on the value of auditing as evidence of compliance in the event of complaints and by developing and providing privacy audit training for organisations.

Review rights for complaint decisions

40 The Australian Government should consider amending the Privacy Act to give complainants and respondents a right to have the merits of complaints decisions made by the Privacy Commissioner reviewed.
### Fair and transparent complaint processes and resolution

41 The Australian Government should consider amending National Privacy Principle 1.3 to require organisations to tell individuals how they can complain to the organisation; and that, if the complaint is not resolved, they can also complain to the Privacy Commissioner or (where relevant) the code adjudicator.

42 The Office will review its complaints handling processes and will consider the circumstances in which it might be appropriate to make greater use of the Commissioner’s power to make determinations under section 52 of the Privacy Act.

43 The Office will also consider measures to increase the transparency of its complaints processes and complaint outcomes.

### Additional powers

44 The Australian Government should consider amending the Privacy Act to:

- expand the remedies available following a determination under section 52 to include giving the Privacy Commissioner power to require a respondent to take steps to prevent future harm arising from systemic issues
- provide for enforceable remedies following own motion investigations where the Commissioner finds a breach of the NPPs
- provide a power for the development of binding codes and/or binding guidelines in cases where there is a strong public interest, where more detailed guidance is warranted or complaints reveal recurrent breaches (see recommendation 7).

### Resourcing implications and complaint handling

45 The Australian Government should consider the strong calls by a wide range of stakeholders for the Office to be adequately resourced to meet its complaint handling functions.

46 The Australian Government should consider amending the Privacy Act to give the Commissioner a further discretion not to investigate complaints where the harm to individuals is minimal and there is no public interest in pursuing the matter.
6 Balancing individual privacy interests with business efficiency

6.1 Introduction

Law and policy

The private sector provisions of the Privacy Act introduced what the then Attorney-General called a 'light touch' approach to privacy protection. They established a co-regulatory regime which was intended to be responsive to both business and consumer needs. This was to be achieved by using high level principles rather than prescriptive rules and by encouraging organisations and industries to develop their own privacy codes.

The legislation also included a number of exemptions, including an exemption for employee records, on the ground this was better dealt with under workplace relations legislation, and an exemption for small business.

Issues

The issues paper considered the balance struck by the private sector provisions between individual privacy interests and business efficiency. It discussed, among other things, the high level principles approach, the costs of compliance, the level of compliance, industry and organisation codes and the small business exemption.

Striking the balance

Submissions are divided on the question of whether or not the private sector provisions strike the right balance between individual privacy and business efficiency. Electronic Frontiers Australia (51) and Xamax Consultancy Pty Ltd (3) suggest that the existing provisions are so inadequate that a new Act that makes a genuine attempt to protect individuals’ privacy is the only solution.

On the specific issue of balance, the Communications Law Centre (72) says there is an overwhelming imbalance between the competing interests of organisations and individuals, where organisations’ interests such as business efficiency clearly outweigh the privacy rights of individuals.

On the other hand, submissions from business are more likely to support the existing regime. Promina Group (34), an insurance and financial services corporation, for example, supports the regime and the approach taken by the Privacy Commissioner and says that this approach creates the right balance.

---

149 Privacy Amendment (Private Sector) Bill 2000 Second Reading Speech House of Representatives Hansard, 8 November 2000, p 22370.
between commercial or business interests and the protection of an individual’s privacy rights.

Similarly, Telstra Australia Ltd (110) states that the Act contains an effective balance between rights of the individual. In its view, this balance could be enhanced by the Office lifting its profile and providing more information about privacy issues to the community.

**Principles or rules**

**Submissions generally support principles based approach**

The submissions that address the issue generally support the principles based approach of the private sector provisions. It is the approach that best allows Australian businesses to adopt practices that are tailored to individual businesses while providing consumers with an assured level of protection150.

It allows each business the opportunity to identify its own business practices and to apply the principles to them151. It provides adequate levels of privacy protection without imposing unnecessary compliance costs on business152.

High level non-prescriptive principles, adequately supported by guidelines and information sheets are the most appropriate way to meet the needs of individuals and businesses. A more prescriptive approach would increase compliance costs without necessarily delivering an improvement to the protection of individuals’ privacy153. The dangers of a more prescriptive system are that the system may be inefficient and/or unworkable in the many business circumstances in which it would apply and, needing ongoing amendment to keep up with technological change, would add to the confusion and compliance costs faced by business154.

Some submissions offer qualified support of the principles. The Australian Chamber of Commerce and Industry (22), for example, agrees with the approach but says that the NPPs themselves are reasonably prescriptive, and that their content and the obligations they impose are onerous.

**Principles may need some illumination**

A few submissions want more than high level principles. They are concerned with what else is in place to illuminate the principles, or to support their operation in practice.

---

150 Microsoft Australia 20.  
151 Victorian Automobile Chamber of Commerce 113.  
152 Vodafone Australia Limited 112.  
153 Insurance Council of Australia Ltd 59.  
154 Chamber of Commerce and Industry of WA (Inc) 77.
The Tenants’ Union of Queensland (69), for example, believes that more specific regulation of tenancy databases is required.\footnote{Tenancy databases are discussed in more detail in Chapter 2.}

The members of a charitable organisation, St Vincent de Paul (117), experience a lack of certainty and need practical guidance on what is permitted and what is not.

### 6.2 Approved Privacy Codes

**Law and policy**

Codes, both industry and organisation, were intended to be a key feature of the privacy regime established by the private sector provisions. The aim of the legislation was, in the words of the then Attorney-General:

‘to encourage private sector organisations and industries which handle personal information to develop privacy codes of practice’ \footnote{Privacy Amendments (Private Sector) Bill 2000, Second Reading Speech, 12 April, House of Representatives Hansard p 15750.}

The Privacy Commissioner may approve a code if, and only if the Commissioner is satisfied of specific matters listed in the Privacy Act. In deciding whether to approve a privacy code, the Commissioner may consider matters specified in guidelines issued by the Commissioner, if any.\footnote{See section 18BB (4) of the Privacy Act.}

Among the matters the Commissioner must be satisfied of is the requirement that the code incorporates all the NPPs or set out obligations that, ‘overall are at least the equivalent’ of all the NPPs.\footnote{See section 18BB (2)(a) of the Privacy Act.}

The Guidelines to the National Privacy Principles, developed by the Office, say that a code has to be reviewed every three years.

Codes are now legislative instruments under the *Legislative Instruments Act 2003*. They are not disallowable by the Parliament. As a legislative instrument, the decision to approve a code is not reviewable under the *Administrative Decisions (Judicial Review) Act 1977*. The decision not to approve one may be reviewable.

**Issues**

The issues paper noted that, despite the expectations at the time the legislation was passed, there have been very few applications for code approval. Only three codes have been approved, and three more are in the
pipeline\textsuperscript{159}. The issues paper listed possible reasons for the apparent lack of interest in developing codes and reasons why an industry or organisation might want to develop one. It also noted perceived inadequacies in the approval process. These include a lack of transparency and the failure of the Privacy Commissioner to publish reasons for approving a code. It suggested a number of possible topics for submission, including:

- the value of codes
- why there have been so few applications
- the effectiveness of the code approval process and
- ways of overcoming problems related to codes.

What submissions say - issues

Overview

Submissions from the three industry groups that have a code throw some light on the code development and approval process. Submissions from other industry groups and organisations, which generally support codes, consider the reasons why there are so few of them. Finally, two submissions from consumer groups consider them from the point of view of consumers.

Insurance Council of Australia

The Insurance Council of Australia (59) supports co-regulation through industry codes because it provides a desirable level of flexibility for business. It looks forward to undertaking its three yearly review of its code in 2005. However, it found the code approval process complex and highly prescriptive. This made it an expensive process, involving costs such as staff time, external legal costs for drafting, extensive consultation with industry, costs of reviewing versions of the Code, implementing compliance systems specific to the Code and, if applicable, fees to an independent code adjudicator.

Clubs Queensland

Clubs Queensland (96) sees its code as an important service to its members. It noted, however, that the code development process was, however, extremely complex and costly because of the generic nature of the Code Development Guidelines issued by the Office. These required Clubs Queensland to consult not only members of clubs but the public generally. It fears that the review of its code will require a substantial administrative and

\textsuperscript{159} Existing codes are; Market and Social Research Privacy Code; General Insurance Information Privacy Code; Clubs Queensland Industry Privacy Code. Codes in development include: Australian Casino Association Privacy Code; Internet Industry Privacy Code; Biometrics Institute Privacy Code.
financial commitment because of the complexity of the process and, if the cost is prohibitive, may tell its members to revert to the NPPs.

**Association of Market Research Organisations and the Australian Market and Social Research Society**

The Association of Market Research Organisations and the Australian Market and Social Research Society (61) state that most major research organisations operate within the framework of the approved industry code. It believes that, on the whole, the Privacy Act works well, providing research participants with appropriate privacy safeguards and helping the industry to differentiate itself from industries with less stringent protection practices.

**Reasons why there are few codes**

**Business perspective**

Most submissions from business support codes in principle. The Real Estate Institute of Australia (13), however, is ambivalent. It expresses concern about the multiplicity of government bodies seeking to use codes to regulate business, thereby shifting a heavy cost burden from government to industry. On the other hand, it believes there are benefits in industry playing a role in developing a code of conduct.

Other submissions from business suggest a variety of reasons why there are only three codes. The Australian Chamber of Commerce and Industry (22) states that the benefits to consumers of an organisation adopting a code, which it sees as a higher standard, do not outweigh the costs to the organisation. In any case, the NPPs are adequate and codes take some time to develop. Coles Myer (60) believes there are few codes because the NPPs work.

A number of submissions focus on the cost and complexity of developing a code. The Australian Direct Marketing Association (67) gives three reasons:

- the approval process is more complex than had been anticipated
- the requirement that codes embody a higher standard than the legislation discouraged organisations from developing and submitting codes and
- advice from law firms favoured the ‘default option’ as less expensive and more resource efficient.

Several submissions say there is little point in developing a code. Privacy Law Consulting Australia (66) sees little benefit in developing and maintaining a code for the majority of organisations and industries. The Royal District Nursing Service (78) agrees, stating that:
‘It is of little or no benefit for an organisation to seek to prepare at its own significant cost and impose on itself a Code that must be of a standard of no less than that imposed under the current legislation.’

In the view of Telstra Corporation Ltd (110), codes will generally only be attractive to industries with specific requirements.

Consumer perspective

The Australian Privacy Foundation (90), whose submission is endorsed by the Consumers’ Federation of Australia (65), is not surprised there has been relatively little take up of the codes option by the private sector. In its view, there is little advantage to businesses in developing or adopting a code. The development and approval process is long and onerous and the inclusion of a complaints handling process effectively privatises costs that would otherwise be borne by government. It is concerned that a proliferation of codes would further confuse the public and detract from privacy awareness building.

The Australian Consumers’ Association (ACA) (15) is also ‘not unhappy with’ the lack of enthusiasm of business for developing and adopting codes having feared that a proliferation of poorly co-ordinated codes could fragment the regulatory landscape to an unacceptable degree. In its view, it would be far better to address the needs of the Office than to create a hothouse atmosphere to artificially encourage industry codes. The ACA also addresses the potential brand argument of codes. It does not see the role of regulation and regulatory processes to confer competitive advantage.

What submissions say - addressing the issues

Although codes have not proved as popular as might have been expected before the implementation of the private sector provisions, submissions show there is support for the concept. Certainly no-one suggests they should be abolished.

Most submissions that make recommendations focus on simplifying the process. The Insurance Council of Australia (59), for example, recommends that the capacity for co-regulation provided by codes should be retained; the approval process, however, should be made less complex and prescriptive. Australian Direct Marketing Association (67) agrees that there is a continued role for codes in the privacy scheme and that the approval process should be simplified. Clubs Queensland (96) recommends that the requirements in relation to the operation and review of a privacy code be simplified.

Telstra (110) recommends, among other things, that the development of codes would be encouraged if the Privacy Act were amended to give the Commissioner a discretion to approve codes with privacy protections not equivalent to those under the NPPs where it was in the public interest to do so.
There was some support for the proposition that the Office should have the power to initiate the development of a code. The Australian Privacy Foundation (APF) (90) says that the Privacy Commissioner should be able to initiate a code. The Australian Bankers’ Association (70), on the other hand, specifically rejects this. The Investment and Financial Services Association Ltd (89) agrees, saying that it should rest with individual companies or the respective industry body.

The APF also makes a number of other suggestions:

- codes should be disallowable instruments
- the Privacy Commissioner should be required to make public a code proponent’s submission dealing with its public consultation process
- the courts should be deemed to have notice of codes in the register kept by the Privacy Commissioner
- the Privacy Commissioner should be able to review any decision of a code adjudicator.

### Options for reform

#### Repeal code provisions

Since the implementation of the private sector provisions, there has been very few applications for approval of an industry or organisation code. This suggests that it may be appropriate to repeal the code provisions. On the other hand, as the value consumers place on their privacy increases and as industry bodies and organisations become more familiar with the notion of privacy, codes may come into their own.

#### Simplify the approval and review process

The legislation gives the Privacy Commissioner the power to approve a code. The processes for developing, approving and reviewing codes are in Office Guidelines. The Office has now had the experience of three years of the operation of the private sector provisions and is in a favourable position to review the Guidelines with a view to simplifying the processes without reducing code standards. Ensuring a code meets the equivalence test can be time consuming and costly both for the code proponent and the Office.

#### Modify equivalence requirement

The law could be amended to allow an industry or organisation, in developing its code, to provide for a lower level of protection in one area and maintain ‘equivalence’ by providing for a higher standard in another. This would give more flexibility in developing a code that met the needs of the industry or organisation while at the same time protecting the interests of consumers.

---

160 Binding codes are discussed in Chapter 5.
the other hand, it would make the Office’s oversight role more difficult and may be confusing for consumers. It could also add to the problems arising out of national consistency and undermine the technological neutrality of the NPPs.

**Commissioner could give reasons for approving a code**

The Privacy Commissioner’s discretion to approve a code is circumscribed by the legislation. There is a broad discretion, however, not to approve one. The legislation does not impose on the Privacy Commissioner an obligation to give reasons for a decision to approve a code, or not to approve, although the Guidelines state that the Commissioner will give reasons for deciding not to. Improved accountability and transparency may require reconsideration of the issue. On the other hand, the scope of the Privacy Commissioner’s discretion is limited, and giving reasons for approval may well have resource implications for the Office.

**6.3 Recommendation: Approved Privacy Codes**

The Office will review the Code Development Guidelines dealing with the processes relating to code approval with a view to simplifying them.

**6.4 Compliance costs**

**Law and policy**

Compliance with the legislation involves a cost burden on organisations. There was the cost of implementing the legislation in the first place, including developing and reordering systems, developing policies and procedures and training staff. There are also ongoing costs. These include the costs of continuous training and the costs of complying with obligations, for example, informing individuals from whom personal information has been collected, seeking consent for use and disclosure of the information for secondary purposes and providing individuals access to their personal information.

**Issues paper**

The issues paper suggested possible suggestions for submissions, including:

- impact on business of compliance with the provisions
- whether the benefits of having a privacy law outweigh the costs to business and
• ways of reducing any unreasonable costs imposed.

What submissions say

Costs are important

Not surprisingly, most submissions on the issue of costs come from business. The Australian Chamber of Commerce and Industry (22) says compliance costs are critically important to the business community and should be of concern to everyone because they are ultimately borne by the broader community. It goes on to say that there has been no significant research on the costs involved in complying with the private sector provisions and, as a result, policy formulation is done in a vacuum. It suggests that an in depth study should be commissioned.

The Investment and Financial Services Association Ltd (89) says that its members report significant disruption and cost with the original implementation but relatively small ongoing compliance costs.

The Australian Consumers’ Association (15) has little sympathy for complaints about compliance costs. It goes on to say that it is difficult to conjure a vision of a more bare-bones privacy framework:

‘There is no required reporting and no mandatory recording. The [Office] has scant investigative powers and none of audit in the private sector . . . [The Act] sets out little more than reasonably sensible data management practice. The [Office] has no power to seek anything other than restitution and so has little capacity to impose direct cost on industry.’

Actual costs

Some submissions outline the steps taken by organisations to comply with the private sector provisions initially and on an ongoing basis, and the costs involved in compliance. The Insurance Council of Australia (59) lists the initial compliance steps:

• developing privacy policies
• incorporating the privacy policy into telephone sales scripts and e-commerce sales facilities
• developing staff training modules and training existing staff
• incorporating privacy laws into systems for administering contracts and managing claims
• developing roles for staff allocated to privacy and the developing the position of privacy officer
• developing procedures for handling complaints and
• developing procedures for handling requests for access.
The most costly aspect of implementation was the systems changes, estimated to cost $10-15 million for its members.

The steps involved in continuous compliance are:

- annual printing of privacy policies
- privacy disclosure in telephone sales (that is, the extra time spent on the telephone)
- training new staff and refreshing existing staff
- continuous improvement of systems
- continuous employee costs of staff allocated to dealing with privacy
- handling complaints and
- handling access requests.

Costs include $1-2 million per annum for telephone sales, $300 000 to $500 000 per annum for staff training and between $5 000 and $50 000 for the handling of each dispute, depending on the complexity of the dispute.

One member of the Investment and Financial Services Association Ltd (ISFA) (89) spent $430 000 on initial implementation and spends $50 000 per annum on ongoing compliance costs. The company has had eight privacy complaints in the last 3 years. Another member of ISFA (89) spent $2.248 million on initial implementation costs.

At Coles Myer Ltd (60), more than 80 people were directly involved in the implementation program across the Coles Myer group. Coles Myer says a conservative estimate of costs in the lead up to the commencement of the provisions would be more than $300 000 in resource costs and systems development.

For the Suncorp Group (35), the set up and implementation cost was approximately $1.2 million.

Commerce Queensland (83) reports that for the National (National Australia Bank and MLC) the changes which, over a three year period cost about $28 million, included

- training
- development and publication of notifications
- numerous consultants
- external legal advice
- establishment of project team
- technology changes and
- establishment of the Australian Privacy Office (3 permanent full time staff).
State and territory legislation increases costs

A number of submissions focus on the additional compliance costs borne by national organisations that are subject to new and inconsistent state and territory health legislation.

The Australian Compliance Institute (16) and a confidential submission both say that the introduction of legislation by the states and territories has increased the compliance burden on business. As each state or territory introduces new legislation there is a new round of costs for businesses.

In the view of the Investment and Financial Services Association Ltd (89), State and Territory health records legislation with its inconsistencies results in increased compliance costs for its member organisations. The ANZ (40) says differing state and territory (workplace surveillance) laws add to compliance costs and complexity.

Costs and benefits

Most submissions from business focus on the costs of compliance rather than the benefits; some, however, acknowledge that there are benefits. A confidential submission says that the benefits are not commercial, but intangible, for example, increased standing with customers who become confident that the business will deal ethically with their personal information. In a similar vein, Fundraising Institute Australia Ltd (52), states that the benefits, community confidence and trust in the industry, outweigh the costs. Telstra (110) agrees:

‘The significant financial cost to Telstra in taking steps to comply with the Privacy Act has been offset by the value to Telstra of the improved systems and processes and from a brand perspective.’

Coles Myer Ltd (60) says that the costs outweigh the benefits to customers, while acknowledging that a simple cost benefits analysis fails to recognise the value of brand equity or public reputation, in which major companies invest heavily.

Change will involve more costs

A number of submissions note that even minor changes at this stage would involve significant costs. A confidential submission says that there is not justification for increasing the cost of compliance for business in this area. Virgin Mobile (Australia) Pty Ltd (26) wants the costs of changes to be weighed up against any perceived benefits. For Optus (98), it is important that the privacy regime is not changed lightly. Even seemingly minor changes can result in significant additional compliance costs for industry. Finally, Telstra (110) says that any significant changes to the NPPs are likely to
increase the cost of compliance and that any changes resulting from the review should be kept to a minimum. Rather, the focus of the review should be on improving the operation of the existing regime.

6.5 Business awareness

Issues

The issues paper acknowledged that high level principles are less amenable to specific direction than a more prescriptive, rule based regime would have been. It noted that the Office has not made many determinations and that there had been few judicial decisions about the private sector provisions. It identified the Office’s role in promoting awareness as an issue to be considered. It suggested, among other things, as possible topics for submissions:

- evidence about current levels of awareness
- strategies for increasing awareness and
- effectiveness or otherwise of the information prepared by the Office.

What submissions say

Overview

Most submissions that address the issue report a relatively high level of awareness of the private sector provisions and of compliance with them. Nevertheless, a number of submissions suggest ways of improving awareness and compliance. Some submissions identify particular contexts in which problems are caused by a misunderstanding of the provisions on the part of business.

Industry generally familiar with provisions

In the experience of Privacy Law Consulting Australia (66) there is a high level of compliance among large organisations as they have allocated resources and implemented policies, procedures and systems to ensure they meet requirements under the Act. There is a significantly lower level of compliance, however, among mid to small size organisations that are covered by the Act. Reasons for this include lack of awareness.

The Credit Union Services Corporation (64) is of the view that industry generally has become familiar with the NPPs and has developed relevant policies. Optus (98) states that Australian industry is committed to addressing privacy issues positively.
On the other hand, the Victorian Automobile Chamber of Commerce (113) found, in a survey of its members in 2002, that knowledge and understanding of information privacy laws was not as thorough as it would have liked. There was confusion as to which law (Commonwealth or State) applied to the business and whether privacy laws conflicted with other obligations, for example, occupational health and safety obligations.

**Some problem areas**

**Bankruptcy**

Submissions identify particular areas where a lack of knowledge of the provisions or a misunderstanding of the obligations they impose give rise to problems. The Insolvency and Trustee Service Australia (25) says that a review of Part X of the Bankruptcy Act conducted in 2003 revealed a substantial level of misunderstanding about privacy obligations.

Some creditors suggested that the Privacy Act prevented them from giving information to the Trustee in Bankruptcy even though it might assist the Trustee’s administration of the estate. It recommends that more should be done to educate the private sector about appropriately using and disclosing personal information. In addition, public confidence in the personal insolvency system should be recognised as an important social interest to be balanced against an individual right to privacy.

**Medical research**

The National Health and Medical Research Council (32) also identifies misunderstanding of the provisions, rather than the provisions themselves, as a cause of confusion in the complex regulatory framework of medical research. It suggests that the Office should design and implement a structured education and communication campaign with the objective of improving stakeholder understanding.

**Dealing with people with a disability**

The experience of the Australian Guardianship and Administration Committee (114) is that there is significant room for improvement in how service providers interpret and apply privacy legislation, especially in relation to people with a disability and their families. It believes that frontline staff implement inflexible policies as to how the provisions should be interpreted and applied and that this gives rise to nonsensical and frustrating situations where common sense solutions should apply. The committee recommends that the Office should divert a significantly greater resource commitment to education and training and that it should publish an information sheet or good practice guide that emphasises the need for a common sense approach, particularly in situations that involve relatively minor issues.
Other

The Police Association (Victoria) (116) states that organisations are not fully conversant with the exemptions to the Act, in particular the law enforcement exemption\textsuperscript{161}.

**How the Office could assist business**

Some submissions suggest ways the Office could assist business in complying with its obligations. The Australian Direct Market Association (67), for example, suggests that the Office should review its communications strategies, particularly with key stakeholder organisations. Business would like to see, it says, effective and comprehensive reporting of rulings complete with the reasoning behind decisions\textsuperscript{162}.

The St Vincent de Paul Society (117) says that charities need clear, practical guidelines.

The Australian Privacy Foundation (90) takes a different approach. It says consideration should be given to requiring:

- significant personal data users to maintain a publicly available management plan
- larger organisations at least to nominate a designated privacy contact officer for contact by the regulator and to publicise contact details and
- larger or significant organisations to have to conduct and report on periodic audits.

**Options for reform**

**Office should conduct a community awareness campaign about business obligations**

There is no doubt that there is a degree of misunderstanding and confusion about the private sector provisions among some business sectors, especially small business. It is not only businesses that are covered by the Privacy Act, but businesses that are not, that are uncertain of their obligations. Many businesses including those who are not covered by the Privacy Act, err on the side of caution in not disclosing personal information in circumstances where it is appropriate that is should be, for example, the amount owing on a utility bill to a carer who wants to pay the bill. The Office could address this gap in awareness.

\textsuperscript{161} The law enforcement exemption is discussed at in Chapter 7.

\textsuperscript{162} Professor Graham Greenleaf 47 argues strongly for reform of the Office’s reporting practices.
**Review Office information sheets**

The Office has published a series of information sheets on a range of topics including codes, privacy obligations for Australian Government contractors and the application of the NPPs to due diligence and completion when buying and selling a business. The consultation process has identified ways in which some of them could be made more useful. There could be a thorough review of the Office’s information sheets with a view to amending them.

**Review strategies for communication with stakeholders**

The Commissioner takes advice from the Privacy Advisory Committee163. The Commissioner also invites people to participate in ad hoc consultative bodies for particular purposes. There is, for example, a reference group for this review. There are, however, other measures the Office could take to ensure it communicates effectively with stakeholders. One such measure could be to establish a privacy contact officer network for the private sector along the lines of the privacy contact officer network in the public sector.

**Impose obligations on organisations to keep records and report**

One way to ensure that organisations continue to fulfil their obligations under the NPPs is to impose obligations on them to appoint a contact officer for contact by the Office, to keep records and to report on their compliance. This could ensure more effective oversight of organisations by the Office. On the other hand, it is not consistent with the principles based approach of the private sector provisions.

**6.6 Recommendations: Business awareness**

48 The Australian Government should consider the benefits of greater business and community awareness of privacy and specifically fund the Office to undertake a systematic and comprehensive education program to raise business awareness.

49 The Office will review existing information sheets and develop information sheets on key issues identified in submissions.

50 The Office will develop strategies for communication with stakeholders, including establishing a privacy contact officer network for private sector organisations.

---

163 The Privacy Advisory Committee is established by section 82 of the Privacy Act. It consists of the Commissioner and up to six other members. Its functions are to advise the Commissioner; to recommend materials for inclusion in guidelines; and, subject to the Commissioner’s direction, to engage in and promote community education and community consultation.
6.7 Small business exemption

Law and policy

Current law

Generally speaking, a ‘small business operator’, that is, a business that has an annual turnover of $3 million or less is exempt from the operation of the private sector provisions. Some small businesses, however, must comply with the provisions. They are small business that:

- are related to a business that has an annual turnover of more than $3 million
- provide health services to people and hold health information about them
- trade in personal information, for example, by buying or selling names and addresses for inclusion on a database, unless it does so with the person’s consent or
- are contracted to provide services to the Australian Government.

In addition, a small business may voluntarily opt-in to be covered by the provisions. Currently 130 small businesses have opted in to coverage.

Finally, the Government may prescribe small business operators, or acts or practices of small business operators, bringing them within the operation of the Act. To date this provision has not been used.

Rationale for the exemption

There are two main reasons for the small business exemption. First, many small businesses do not have significant holdings of personal information. They may have customer records used for their own business purposes; however, they do not sell or otherwise deal with customer information in a way that poses a high risk to the privacy interests of those customers.\footnote{Privacy Amendment (Private Sector) Bill 2000 Second Reading Speech, Hansard House of Representatives, 8 November 2000, pp 22370-1.}

Secondly, it is necessary to balance privacy protection against the need to avoid unnecessary cost on small business.\footnote{Privacy Amendment (Private Sector) Bill 2000 Second Reading Speech, Hansard House of Representatives, 12 April 2000, p 15752.}

Issues

The issues paper considered the operation of the small business exemption and suggested possible topics for submissions:
• whether the exemption reduces the compliance burden on small business
• whether the benefits of the exemption outweigh the disadvantages for business and for individual
• whether the provisions are clear about to whom the exemptions applies
• whether the $3 million or less threshold is still appropriate and
• any other issues raised by the exemption and ways of overcoming them.

What submissions say

Overview

Submissions are roughly evenly divided between retention of the small business exemption and repeal. Submissions favouring retention generally come from businesses and business organisations. Submissions favouring repeal come from consumer groups and also from some businesses and a charity organisation. Some submissions that favour retention suggest that the definition should be changed.

Repeal the exemption

A number of submissions that favour repealing the exemption focus on the potential for confusing consumers. The Australian Consumers’ Association (15) says it raises serious practical difficulties for consumers who do not usually know what the annual turnover of a business is and therefore if they can make a complaint or not. Electronic Frontiers (51) notes that individuals are rarely in a position to know whether or not the business they are dealing with is a small business for the purposes of the Privacy Act since annual turnover is not usually published. As the Australian Privacy Foundation (90) says, there is no easy way for consumers to know the turnover of a business and therefore whether or not it is subject to the Privacy Act.

Fundraising Institute Australia Ltd (52) notes that not only is the exemption confusing it has the potential to undermine public confidence about the protection of personal information. The Australian Direct Marketing Association (67) opposes exemptions that cause confusion in the minds of consumers and undermine confidence in the effectiveness of privacy protection.

Some submissions claim that some of the most privacy intrusive activities are performed by small businesses, even sole traders, including private detectives, debt collectors, internet service providers and dating agencies. They also claim some, for example internet service providers, may hold significant personal information, including sensitive information.

\^166\ See, for example, Consumer Credit Legal Centre (NSW) Inc 62; Consumers Federation of Australia 65; Australian Privacy Foundation 90.

\^167\ Fundraising Institute Australia Ltd 52
Fundraising Institute Australia Ltd (52) says the costs argument is not enough to justify retention; and, in any case, says the Australian Consumers’ Association (15), the cost burden of compliance is not significant.

At the very least, in the view of the Australian Privacy Foundation (APF) (90), the core requirements should apply to all businesses, large and small:

‘The core requirements of the NPPs - being open about the use of personal information, handling it in accordance with reasonable expectations, and keeping it secure, should apply to all organisations. It would however be reasonable to exempt many smaller businesses from any formal requirements to take particular actions, in advance of enquiries’.

In the APF’s view, small businesses that collect and handle personal information for a purpose that is or should be obvious should not have to give specific notices under NPPs 1.3 and 1.5. They should, however, be required to answer enquiries (NPP 5) and give access and make corrections on request (NPP6). They should be able to be held accountable after the event for their collection and use of personal information and for any data quality or security breaches.

Finally, the exemption costs the members of at least one industry organisation. The Australian Collectors Association, Institute of Mercantile Agents, Australian Institute of Credit Management (115) say that debt collectors who are contractually bound by their clients not to outsource to non-compliant companies must send city based staff to service regional areas. In their view, this forces up their costs to unreasonably high levels.

**Retain the exemption**

Most submissions that favour retaining the exemption do so on the basis of the costs arguments, that is, that the costs of compliance would be too great for small business to bear.

Regulatory ‘red tape’ and compliance costs have a major detrimental effect on the viability of small businesses in Australia, according to the Real Estate Institute of Australia (13). The Victorian Automobile Chamber of Commerce (113) says that small businesses would be greatly disadvantaged if they had to comply with the private sector provisions as their competitiveness and profitability would be reduced. The Housing Industry Association Ltd (106) says that removing or diluting the exemption would impose unnecessary significant costs on small businesses in the housing sector, including the more than 350 000 independent contractors that work in the residential building sector.
Certainly there should be no change in the absence of a substantial body of evidence suggesting there is a problem, in the view of the Chamber of Commerce and Industry of WA (Inc) (77).

The Australian Chamber of Commerce and Industry (22) estimates that there are about one million businesses in Australia currently exempt and that the bare minimum costs of their establishing a simple privacy regime would amount to a total of $2.4 billion, or about 0.3 per cent of gross domestic product.

**Change the definition of small business**

Some submissions suggest changing the definition of small business for the purpose of the exemption. The Australian Information Industry Association (43) suggests changing it to that used by all governments to describe small and medium enterprises. The Association of Market Research Organisations and the Australian Market and Social Research Society (61) notes that the current definition is at odds with that used by the Australian Bureau of Statistics and the Australian Taxation Office.

A number of submissions favour retaining turnover as the basis of the definition but say it should be increased to $5 million\(^{168}\).

Other submissions consider focussing on the level of risk. The Communications Law Centre (72) suggests including within the operation of the Act industries that pose a particular risk. It identifies the internet/e-commerce as one where small internet businesses are able through the use of privacy invasive technologies to collect efficiently and easily a large amount of personal information about many individuals.

The Consumer Credit Legal Centre (NSW) Inc (62) and the Consumers’ Federation of Australia (65) nominate telecommunications and finance as industries once dominated by large companies but now including many small businesses.

In the view of Electronic Frontiers Australia Inc (51), at the very least, all small businesses involved in the telecommunications and internet services sector must be required to comply with the NPPs. It says there are two reasons for this. First, the limited privacy protection provisions of the Telecommunications Act do not cover the collection of personal information at all. Secondly, individuals have less control and rights in relation to the collection, use and disclosure of their personal information by small businesses in the telecommunications sector than they did before December 2001 when the ACIF industry code, containing substantially the same provisions as the NPPs and enforceable by the Australian Communications Authority, was...

\(^{168}\) See, for example, Australian Chamber of Commerce and Industry 22; Commerce Queensland 83; Queensland Retail Traders and Shopkeepers Association 125. See also Victorian Automobile Chamber of Commerce 113.
deregistered by the Authority. That code did not contain a small business exemption.

**Other issues**

Some submissions raise other issues relating to the small business exemption. The Consumer Credit Legal Centre (NSW) Inc (62) points out that a debtor who borrows money from a large financial institution that is covered by the private sector provisions may find himself or herself dealing with a debt collector who, being a small business, is not. The privacy protection he or she may have expected when entering the loan may no longer exist.

Privacy Law Consulting Australia (66) fears that it is possible that small businesses that are not bound by the Act may give the impression that they are by having a privacy statement, perhaps on their website, to the effect that: ‘We comply with the Privacy Act’. To avoid confusion, it may be desirable to require the business to state that is not bound by the Act, but that it chooses to do so.

In the view of Telstra Australia Ltd (110), which ensures compliance on the part of its small business contractors by contract, the voluntary opt-in for small business should be better promoted.

**Options for reform**

**Retain the exemption as is**

The main argument in favour of retaining the exemption is that the cost of compliance for small business would be too great if the exemption were abolished. It could also be argued that any change is likely to result in increased compliance costs. There does not appear to be evidence of large scale misuse of personal information by small businesses as a whole such that would warrant the removal of the exemption.

**Abolish the exemption**

The main reasons for abolishing the exemption are its capacity to confuse consumers and the fact that it does not differentiate adequately between those businesses that hold significant personal information and those that do not. On the other hand, as many small businesses do not hold much personal information it would in fact make little difference to them. Nevertheless, small business may find the costs of implementation and the additional red tape unduly burdensome. Finally, the exemption is a barrier to EU adequacy.
Retain the exemption and change the threshold

There is no apparent reason why the threshold should be a turnover of $3 million. Similarly, there are no compelling policy reasons why it should be increased or decreased. The turnover criterion has been criticised as being meaningless for consumers and as an irrational indicator of size. It is not commonly used as a way to define small business.

Retain the exemption and change the definition

A business's annual turnover is not generally known. The Australian Bureau of Statistics (ABS) defines small business (excluding agricultural businesses) as businesses with less than 20 employees. Although arbitrary, a definition of small business in terms of the number of employees rather than annual turnover may be more easily understood by consumers and other interested parties. If the definition is expressed in terms not of the particular number of employees but the definitions used by the ABS, from time to time, the need to amend the Act each time the ABS definition is changed is avoided.

Impose core requirements of NPPs on small businesses

A small business holding very little personal information is able to use or disclose it in a way that causes significant damage to an individual. The exemption could be modified to impose the core requirements of the NPPs on all businesses and to exempt them from others. They would be accountable for their actions only in the event of a complaint. This would add to the compliance burden of small businesses, but it would not be as onerous as if the exemption were to be removed completely.

Retain the exemption and include high risk sectors within the operation of the Act

It is sensible and consistent with the policy underlying the Act to include within the operation of the private sector provisions small businesses that belong to high risk sectors in that they handle a lot of personal information, including sensitive information, and give rise to a lot of complaints. To date, the evidence suggests telecommunication service providers and tenancy databases are such sectors.

There are two means by which small businesses that are in a high risk sector could be included: by amending section 6D (4), or by the Attorney-General using the power to prescribe the sectors under section 6E.

The use of the power to prescribe by regulation avoids amending the Act and sets a precedent for the inclusion of other sectors that may become high risk. The power has always existed. It has not yet been used but it was envisaged...
that the Attorney-General would use it in appropriate circumstances to bring into coverage under the Act industries and organisations that collect and use a lot of personal information.

**Remove the consent provision**

Small businesses that trade in personal information are not exempt from the operation of the Privacy Act. If, however, the individual consents to the collection or disclosure of the personal information then the business remains a small business and is exempt\(^{169}\). This is clumsy and complicated. There is a considerable lack of certainty for small businesses who trade in personal information because it is not clear whether only a single failure to gain consent would change the status of the organisation. The provision could be removed.

### 6.8 Recommendations: Small business exemption

51 The Australian Government should consider retaining but modifying the small business exemption by amending the Privacy Act so that the definition of small business is to be expressed in terms of the ABS definition, currently 20 employees or fewer, rather than annual turnover.

52 The Attorney-General should consider using the power to prescribe under section 6(E) of the Privacy Act, the tenancy databases and telecommunications sectors including Internet Service Providers and Public Number Directory Producers as businesses to be covered by the Act. (See recommendations 9 and 15.)

53 The Australian Government should consider amending the Privacy Act to remove the consent provisions (sections 6D(7) and 6D(8)).

---

\(^{169}\) See sections 6D(7) and 6D(8) of the Privacy Act.
6.9 Private sector contracting

Law and policy

Many organisations outsource some of their functions or activities. Some of these may involve handling personal information, including sensitive information, collected by the organisation. It might, for example, include health information. There is no clear obligation in the NPPs (unlike the IPPs) that would require the organisation to ensure that the contractor uses the personal information only for the purposes for which it is given and to keep it secure.

The contractor may not itself be bound, for example, if it is a small business. It may not be clear to consumers that they are dealing with a contractor because organisations often prefer the contractor to identify itself under the organisation’s corporate name. The Privacy Act does not make any specific provision for a contractor to be regarded as acting as an agent for the organisation it is providing services for. It is generally regarded as a separate entity. This means the contractor collects personal information from the organisation, which discloses it to the contractor.

Issues

The issues paper noted that as the Privacy Act does not provide for the existence of an agency relationship between an organisation and a contractor, the contractor needs the consent of each individual to collect sensitive information, for example, health information, from the organisation. Similarly, a contractor that is collecting information for an organisation to whom it has contracted its services may need to identify itself under NPP 1.3 as being a separate organisation, and may need to get the consent of the individual from whom it collecting sensitive information to disclose the information to the organisation on whose behalf it is collecting it. The issues paper suggested possible topics for submissions:

- adequacy of the private sector provisions in protecting individual privacy where organisations contract out their functions or activities
- impact of the provisions on businesses when they contract out functions or activities that involve handling personal information, particularly sensitive information and
- ways that issues that arise might be resolved.

What submissions say

Existing regime is working

Some submissions say that the existing regime is working and that no amendment is needed. Telstra Corporation Ltd (110), for example, says that any uncertainty has been addressed through guidelines and information sheets. Vodafone Australia Ltd (112) says that potential problems are dealt
with by using contracts to bind service providers to comply with privacy law. It does not want this way of ensuring privacy obligations are complied with restricted in any way.

**Distinction between data controllers and data processors**

A number of submissions outline the ways they use contractors. The Australian Direct Marketing Association (ADMA) (67) says, for example, that it is extremely common place in nearly all industry sectors for organisations to engage a third party service provider or outsource agency to conduct a business operation on its behalf. It is also commonplace for a third party contractor or outsource agency to require access to an organisation’s customer records and other personal information in order to perform such operations. The outsourced activities may include:

- engaging a mailing house, call centre or email/SMS service provider to distribute communications
- engaging data quality, data enhancement or analytical services and
- contracting a company to undertake data storage functions.

In ADMA’s view, it is unduly onerous to impose the collection and disclosure requirements on both the organisation and the service provider. It is also unnecessary because one is merely performing an operation or processing data on behalf of the other. They should not continue to be regarded as two separate entities for the purposes of the NPPs. Instead, the European Union approach, which recognises the distinction between an organisation, a ‘data controller’, and a third party service provider, a data processor, should be adopted.

This distinction is made by a number of submissions, including the Law Council of Australia (36) and the Australian Information Industry Association (43). A confidential submission notes that there is confusion as to whether each contractor, as well as the principal organisation, should disclose its name and function to an individual who is providing personal information. All three submissions recommend that the distinction should be recognised to allow business to achieve its objectives efficiently.

**Relationship of principal and agent**

Some submissions approach the issue from an agency law perspective. These include the Australian Finance Conference (63) and Optus (98). The Australian Finance Conference, for example, takes the view that the law of agency makes unjustifiable the conclusion that when an organisation discloses information to a third party contractor it is ‘disclosing’ to a separate ‘organisation’. In its view the reference in the Office’s Information Sheet 8 - Contractors to a ‘particularly close relationship’ encompasses the principal/agent relationship. In any case, its members have established their compliance programs on this basis and would oppose moves to change this
accepted understanding. On that basis, it recommends that there be no change to Information Sheet 8.

Promina (34) takes a narrow view of *Information Sheet 8 – Contractors*. It describes the circumstance where an insurer paying claims may decide to outsource its cheque printing process to a third party. Strict contractual provisions prohibit the contractor from using the personal information for any other purpose than to produce the cheques. In Promina’s view, *Information Sheet 8 – Contractors* should be amended to support the position that there need be no further privacy disclosure in such a case.

### Options for reform

#### Amend NPP 4

NPP 4 requires an organisation to take reasonable steps to protect personal information it holds. It does not deal specifically with what should happen when information is given to a contractor. IPP 4 does. It requires the organisation to ensure ‘everything reasonably within the power of the record-keeper is done to prevent unauthorised use or disclosure’. NPP 4 could be amended to strengthen it in line with IPP 4. This puts the obligation on the contractor. It addresses the problems that arise when a contractor subcontracts to a small business that is not covered by the Act.

#### Business should ensure contact imposes relevant obligations on contractors

One way an organisation can ensure that a contractor protects the personal information the organisation has given it for the purposes of performing an operation on behalf of the organisation is to impose the obligations by contract. The Office could amend its Guidelines to this effect.

#### Amend Information Sheet 8

There seems to be some confusion as to what exactly *Information Sheet 8 – Contractors* means. The Office should amend it to clarify issues relating to private sector contracting.

#### Distinguish data controller and data processor

The private sector provisions could be amended to distinguish between data controllers and data processors and to amend the NPPs accordingly. This would overcome the particular issue but would have an impact on the operation of the Privacy Act.
6.10 Recommendations: Private sector contracting

54 The Australian Government should consider amending NPP 4 to impose an obligation on an organisation to ensure personal information it discloses to a contractor is protected.

55 The Australian Government should consider, in the context of the wider review of the Privacy Act, (see recommendation 1) whether there should be a distinction between data controllers and data operators.

56 The Office will amend the Guidelines to the National Privacy Principles to clarify that businesses that give personal information to contractors for the purpose of performing a function on their behalf should impose contractual obligations on the contractor to take reasonable steps to protect the information.

6.11 Due diligence on sale or purchase of business

What is due diligence?

'Due diligence' is the term used to describe the process that a prospective purchaser of a business undertakes to assess the value of a business’ assets and liabilities. The due diligence process may involve the disclosure and collection of a number of different types of personal information including:

- employee information
- customer information
- information about trading partners and business associates and;
- marketing files.

Information Sheet 16

As a result of inquiries from organisations buying and selling businesses and engaging in due diligence processes, the Office published Information Sheet 16 Application of key NPPs to due diligence and completion when buying and selling a business. Information Sheet 16 advises buyers and sellers about complying with their obligations under the Privacy Act.

A vendor organisation:

- cannot disclose personal information unless the disclosure is permitted under NPP 2 and
must consider the requirements of NPP 4 (data security) when personal information is disclosed and conduct the sale in a way that reasonably protects the privacy of the individuals whose personal information has been disclosed.

A prospective purchaser organisation:

- must consider its obligations in relation to the collection of personal and sensitive information (NPP 1 and NPP 10) and
- must be aware that there may be limitations on how it can use and disclose that information (NPP 2) and that it may need to comply with reasonable restrictions imposed by the vendor organisation.

Issues

The issues paper suggested that it may be difficult to determine how the NPPs apply to the disclosure of personal information during the course of due diligence.

‘Depending upon the nature of the business being sold, due diligence may involve disclosure of personal information about key employees or even sensitive information, for example, health information, about employees or clients’.

What submissions say

Few submissions address the issue of due diligence in the buying and selling of a business. There have been no complaints to the Office about a breach of privacy during a due diligence process. Two submissions address the content of Information Sheet 16. The Insurance Council of Australia (ICA) (59) notes that the relationship between the vendor and the purchaser in the Information Sheet is somewhat artificial and that, in reality, business practice requires extensive amounts of information, including personal information, to be divulged between the parties.

The ICA suggests that Information Sheet 16 consider and address the following issues:

- the requirements for the transfer of personal information which are required or authorised by law during a sale and purchase of a business and
- the disclosure of large amounts of personal information is vital for a purchaser to make a decision on price and financial viability.

A confidential submission suggests that Information Sheet 16 should consider the issues one would consider when transferring (as opposed to buying) a portfolio of business, such as when a portfolio of insurance business is transferred from one insurer to another.
Options for reform

Amend NPPs to take account of due diligence

Businesses are bought and sold. Businesses that hold sensitive personal information are bought and sold. Due diligence occurs. It may be technically a breach of the NPPs. The key NPPs are NPPs 1, 2 and 10. The buying and selling of medical practices or insurance companies, for instance, which requires the transfer of sensitive health information would require consent under NPP 10, unless one of the other exceptions in NPP 10.1 applied, for example, the transfer is required by law. It is not practical, and may not be possible, to require an organisation in the process of due diligence to gain the consent of everyone whose personal information is transferred. The relevant NPPs could be amended to take onto account the practical realities of due diligence.

Amend Information Sheet 16

Some submissions have made suggestions as to how Information Sheet 16 might be clarified. The issue is complex and the information published by the Office should be as clear and as comprehensive as possible.

6.12 Recommendation: Due diligence

The Australian Government should consider amending the NPPs to take into account the practice of due diligence.
7 Balancing individual rights and other social interests

7.1 Media exemption

Introduction

One of the competing social interests identified in the private sector provisions is the free flow of information. One of the ways the legislation promotes the free flow of information is to exempt the acts and practices of media organisations in the course of journalism from the application of the provisions. This exemption applies where such a media organisation is publicly committed to observing published standards that deal with privacy in the context of the activities of a media organisation.

Law and policy

Privacy Act

‘Media organisation’ is defined under section 6(1) of the Privacy Act. The term refers generally to organisations whose activities consist of or include the collection, preparation for dissemination or dissemination of news, current affairs, information or documentaries.

The media exemption is outlined in section 7(B)(4) of the Privacy Act:

(4) An act done, or practice engaged in, by a media organisation is exempt for the purposes of paragraph 7(1)(ee) if the act is done, or the practice is engaged in:

(a) by the organisation in the course of journalism; and
(b) at a time when the organisation is publicly committed to observe standards that:

(i) deal with privacy in the context of the activities of a media organisation (whether or not the standards also deal with other matters); and
(ii) have been published in writing by the organisation or a person or body representing a class of media organisations.

Although, it is not strictly part of the media exemption, it is worth noting that journalists are also exempt from revealing their confidential sources. Section 66(1A) states:

For the purposes of subsection (1B), a journalist has a reasonable excuse if giving the information, answering the question or producing the document or

---

record would tend to reveal the identity of a person who gave information or a document or record to the journalist in confidence.

**Broadcast Media**

Under the *Broadcasting Services Act 1992*, the industry group representing licensees in each section of the broadcasting industry is responsible for developing a code of practice applicable to that section. Privacy provisions are included in these codes of practice\(^{171}\). The Australian Broadcasting Authority (ABA) (19) submits:

> ‘while the privacy provisions vary somewhat across the various broadcasting codes, all reflect the core principle which underlays media regulation in Australia and internationally, i.e. that use of private material in broadcasts has to be warranted in the public interest’.

The industry codes are developed in consultation with the Australian Broadcasting Authority (ABA) and, once approved, are included on the ABA’s Register of Codes. The ABA includes on this Register codes that are endorsed by a majority of industry, provide adequate community safeguards and provide adequate opportunity for public comment.

The ABA has created a draft set of guidelines dealing with privacy issues. A number of other privacy related laws which broadcast media organisations must adhere to is provided in Attachment A Appendix 1 to the Australian Broadcasting Authority submission (19).

**Enforcement**

The ABA may impose a licence condition requiring a broadcaster to comply with a code of practice\(^{172}\). Failure to comply with a licence condition is an offence under section 139 of the *Broadcasting Services Act 1992*. In addition to this, the ABA can impose program standards that apply to all broadcasters in a sector where the code of practice has failed to provide appropriate community safeguards\(^{173}\).

---

\(^{171}\) Commercial Television Code of Practice; Commercial Radio Codes of Practice; Subscription Television Broadcasting Codes of Practice; Community Broadcasting Codes of Practice; ABC Code of Practice (which applies to Television and Radio); SBS Codes of Practice

\(^{172}\) Section 43 *Broadcasting Services Act 1992*

\(^{173}\) Section 125 *Broadcasting Services Act 1992*
Print media

Print media in Australia is regulated by the Australian Press Council. The Australian Press Council is a self-regulatory body that deals with print media, including all commercially available newspapers and magazines and the internet sites of its publisher members within Australia. It was established in 1976 with two main aims:

- to preserve the traditional freedom of speech, and of the press, within Australia by keeping a watch on developments which could threaten such freedoms and
- to ensure that the free press acts responsibly and ethically, by providing a forum to which anyone may take a complaint concerning the press.

The Australian Press Council consists of 21 members, representing the publishers, journalists and members of the public, and is chaired by an independent Chairman.

Principle number three of the Australian Press Council principles deals with privacy. It states:

‘Readers of publications are entitled to have news and comment presented to them honestly and fairly, and with respect for the privacy and sensibilities of individuals. However, the right to privacy should not prevent publication of matters of public record or obvious or significant public interest’\(^\text{174}\).

Enforcement

The Secretariat of the Australian Press Council takes a mediative approach to dealing with complaints with a focus on non-legalistic, accessible and informal processes. If asked to adjudicate, the Australian Press Council holds a hearing of its Complaints Committee, which always has a majority of Public Members, and which makes a recommendation to the Council. The Australian Press Council has no punitive power beyond that of announcing its findings. Its authority stems from the willingness of publications to admit mistakes publicly by printing all adjudications arising from complaints against them. The Australian Press Council’s website states:

‘The industry takes the Council seriously. The proprietors voluntarily finance the Council’s operations and co-operate with it in mediating and processing complaints. An overwhelming majority of adjudications is published prominently’\(^\text{175}\).

\(^{174}\) Australian Press Council, Principle 3, which can be found at http://www.presscouncil.org.au/pcsit/complaints/sop.html

Issues

The issues paper noted that the wording of the media exemption is broad and undefined, is unspecific in relation to the level of standards to which a media organisation must commit itself, and has no requirement that there be a means of enforcing such standards. Another concern raised was that the terms ‘in the course of journalism’ and ‘media organisation’ are yet to be the subject of judicial consideration. The issues paper noted, however, that the Office has received few enquiries or complaints involving media organisations or journalistic activities and suggested that the current exemption may therefore strike an appropriate balance between privacy and the desirable free flow of information.

In particular, the issues paper asked:

- whether the operation of the media exemption is striking the appropriate balance between the free flow of information and individual privacy
- whether the current formulation of the media exemption covers the right organisations and the right activities and
- measures to address any issues that are arising in relation to the media exemption.

What submissions say – issues

A small number of submissions comment on the media exemption. Of these about half report that they either support the exemption or are comfortable with it. The majority of submissions that raise concerns about the media exemption are from health organisations.

Inappropriate reporting of health information

The Australian Medical Association (AMA) (29) argues that the media has a significant capacity to violate privacy and cause harm to patients and should be regulated in a stronger way. It cites a real example of a privacy violation caused by a media organisation reporting on the admission of a person to hospital for psychiatric care:

‘The media invasion of a particular (psychiatric) facility in Sydney severely disrupted the delivery of clinical care and resulted in other patients avoiding admission because they were concerned about the risk of being photographed by reporters covering the story’.

The AMA argues that an appropriate balance is not met by the current exemption. The AMA argues that at present, public curiosity is afforded greater protection than an individual’s right to privacy.

176 For example, Australian Consumers Association 15; Fundraising Institute Australia Ltd 52; Telstra 110
The Mental Health Privacy Coalition (58) echoes the concerns raised by the AMA and requests that media be able to report only limited information about an individual’s healthcare. The Mental Health Privacy Coalition argues that if an individual’s information is of importance to the public interest, the media should apply for permission from the Privacy Commissioner to report on such matters.

St John’s Ambulance Service Australia (97), while acknowledging the balance between informing the public and respecting privacy is difficult to achieve, expresses its concerns with the media’s access to, and reporting of, information from coronial hearings. It states that occasionally inaccurate reporting causes unnecessary distress to people involved in coronial hearings as well as raising ‘undue alarm amongst the public’.

**Inadequate enforcement**

The ABA (19) submission states that it lacks appropriate sanctions (what it calls middle range sanctions) that would allow it to actively enforce the privacy provisions in broadcasting codes of practice. When a breach occurs, the ABA is limited to informing the media organisation and extracting commitments from broadcasters about code training and disseminating the ABA’s breach findings amongst staff. The ABA (19) also states it has found a pattern of repeat offending privacy related breaches in commercial television (though no pattern existed in radio).

The Australian Privacy Foundation (90) criticises the Australian Press Council and Broadcast Media codes. The Australian Privacy Foundation (90) argues that the codes only pay ‘lip service’ to privacy and are ‘widely regarded as ineffectual’.

FreeTV Australia (46) argues that the industry codes of practice are specifically designed to balance the media’s role of informing the public about matters of public interest and protecting individual privacy. FreeTV Australia (46) actively argues in favour of maintaining the media exemption. It states:

‘the Australian media are subject to a wide range of Federal and State laws which provide protection against inappropriate or unfair means of gathering or disclosing personal information and images. These include the laws of trespass, nuisance, breach of confidence, defamation, malicious falsehood, contempt, the use of listening devices and the myriad of laws restricting reporting of specific matters such as national security, adoption, juries, and particular court proceedings’.

**Exemption is too broad**

The Australian Privacy Foundation (APF) (90) argues that the media exemption is too broad and could effectively be claimed in relation to any information that is ‘published’. While the activity must be ‘in the course of journalism’ to qualify for the exemption, the fact that ‘journalism’ is not defined
adds to this criticism. It goes on to argue that the exemption should be narrowed to focus on the public interest role of news and current affairs and that the media exemption should only apply when:

‘(a) the privacy standard is a ‘a bona fide attempt to protect privacy from media intrusions (assessed as such by an independent arbiter) (b) is enforced in some effective way and (c) is generally observed by the media organisation’.

Criticism is also levelled at the requirement in the exemption for a media organisation to commit to a published media code of practice. The APF (90) expresses dissatisfaction with this provision arguing:

‘As there are no criteria for these standards, or provision for review of them, the condition is effectively worthless…Current industry self regulation – including the Press Council and broadcast media codes of practice, only pay lip service to privacy and are widely regarded as ineffectual’.

The APF (90) disputes the fact that the low level of complaints and enquiries received by the Office indicates a general satisfaction with the media exemption, suggesting instead that the low level of complaints and enquiries is better explained by:

‘a widespread and correct view that media are effectively above the law in relation to privacy – unless individuals have the resources to pursue defamation or other common law actions’.

**Other issues**

The exemption applies if a media organisation is publicly committed to observe standards that deal with privacy (section 7B(4)(b)(i)). In interpreting this provision, it is uncertain whether the Privacy Act enables the Commissioner to determine whether a code provides adequate protection or not.

**Options for reform**

**Remove exemption**

Although there are concerns that the media can be intrusive, there is a general recognition that sometimes these intrusions may be justified in the public interest. All submissions recognise that the media has an important role to play in informing the public. The Office also notes that it receives very few enquiries and complaints about media organisations. There is a strong public interest in having a free flow of information. Given there is no strong evidence that there are major concerns about the way the exemption is operating, removing the exemption would appear to be unnecessary.
Clarify whether the Privacy Commissioner can decide whether or not a standard deals adequately with privacy

The media exemption applies when a media organisation ‘is publicly committed to observe standards that deal with privacy in the context of the activities of a media organisation’ 177. It is not clear if this section enables the Commissioner to decide whether or not the standard deals with privacy in an adequate way in the course of establishing whether or not a media organisation is publicly committed to a standard.

This provision could be amended to establish criteria by which the Privacy Commissioner could measure whether the standards adequately ‘deal with’ privacy.

Define the meaning of ‘in the course of journalism’, and clarify the meaning of ‘media organisation’

The media exemption applies ‘if the act is done, or the practice is engaged in by the organisation in the course of journalism’ 178. The Privacy Act does not define the meaning of the term ‘in the course of journalism’. In order to ensure the exemption focuses on news and current affairs, as is in the public interest, the term ‘in the course of journalism’ could be defined and the broadly defined term ‘media organisation’ could be clarified.

Greater guidance

The Office could work with the ABA and media bodies to provide more definitive guidance to media organisations on appropriate levels of privacy protection in privacy standards for media organisations, and how to implement such standards. Greater guidance could be given to ensure that the media sector is aware that the media exemption is not a blanket exemption. Rather, the exemption applies only if the media organisation is publicly committed to observing a privacy code that is published in writing by the organisation.

Require media bodies to consult with Privacy Commissioner when developing codes

Currently, it is not clear that the privacy standards developed for the media are adequate or whether the standards are being implemented. Concerns have also been raised in relation to how health information and especially mental health information is reported. There is particular concern that patients will avoid seeking mental health treatment for fear of the media attention they may attract. It is far less likely that the public interest in having

177 See section 7B(4)(b)(i) of the Privacy Act.
178 See section 7B(4)(a) of the Privacy Act.
a free flow of information will outweigh a person’s right to privacy when it comes to the reporting of health information.

The Privacy Act (and/or the Broadcasting Services Act) could be amended to require the ABA and media bodies to consult with the Privacy Commissioner when developing a code or guidelines dealing with privacy. Requiring media regulators such as the ABA, and media bodies, to work with the Office when developing codes would ensure that media organisations are committed to standards that adequately deal with privacy. Such codes could provide guidance on how media organisations report on matters such as health information.

### 7.2 Recommendations: Media exemption

58 The Australian Government should consider amending the Privacy Act so that:

- the Australian Broadcasting Authority (ABA) and media bodies must consult with the Privacy Commissioner when developing codes that deal with privacy and
- the term ‘in the course of journalism’ is defined and the term ‘media organisation’ is clarified.

59 The Office will, in conjunction with the ABA, provide greater guidance to media organisations as to appropriate levels of privacy protection, especially in relation to health issues, and make organisations aware that the media exemption is not a blanket exemption.

### 7.3 Medical research

#### Law and Policy

There is a social interest in enabling medical researchers to have access to health information in certain circumstances. The Privacy Act is not intended to restrict important medical research. While health information, being sensitive information, is generally afforded extra protection under NPPs 2 and 10, the NPPs recognise the desirability of medical research by enabling health information to be collected, used and disclosed in certain circumstances without consent. Where health information is being collected, used and disclosed for the purpose of research, provided certain criteria are met, the NPPs enable such research to proceed.

#### NPPs

The relevant NPPs in this context are NPP 2.1(d), NPP 10.3 and NPP 10.4.
In limited circumstances, NPP 2.1(d) allows uses or disclosures of health information for research purposes, or for the compilation or analysis of statistics, without consent, where these activities are relevant to public health or public safety. That is, the research must be about, or the statistics related to, public health or safety. Health information may be used or disclosed without consent for these purposes, only if:

- the activities cannot be undertaken with de-identified information and they are relevant to public health and safety
- seeking consent is impracticable
- the activities are carried out in accordance with guidelines that are developed by the National Health and Medical Research Council (or a prescribed authority) and are approved by the Privacy Commissioner, and
- for disclosure - the health service provider reasonably believes that the organisation to which they disclose will not further disclose the health information or any personal information derived from it.

Under NPP 10.3, an organisation may collect health information about an individual if the collection is necessary for:

- research relevant to public health and safety or
- the compilation or analysis of statistics relevant to public health or safety
- the management, funding or monitoring of a health service and
- where collection of information that does not identify the individual cannot be obtained.

In such instances, the information must be 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 approved by the Commissioner under section 95A.

If an organisation collects information under NPP 10.3, then it must take reasonable steps to permanently de-identify the information before it discloses it (NPP 10.4).

The Office has an information sheet on handling health information for research and management\(^{179}\).

**Section 95A guidelines**

Guidelines approved by the Privacy Commissioner under s 95A of the Privacy Act 1988 have been developed by the National Health and Medical Research Council.\(^{179}\)

Council (NHMRC)\textsuperscript{180}. In approving the guidelines the Commissioner must apply a public interest test\textsuperscript{181}.

The guidelines provide a framework to ensure privacy protection of health information that is collected (under NPP 10.3), or used or disclosed (under NPP 2.1(d)) in the conduct of research and the compilation or analysis of statistics, relevant to public health or public safety, and in the conduct of health service management activities. Under the guidelines, Human Research Ethics Committees (HRECs) are required to approve research or statistical activities that involve the collection, use or disclosure of identifying health information, and health service management activities that involve the collection of identifying health information.

In line with NPP 10.3, the guidelines only require HREC approval where the activity is to be conducted without consent from the individual concerned. A HREC may only approve such research where it determines that the public interest in the proposed research, statistical or health service management activity substantially outweighs the public interest in the protection of privacy.

The NHMRC has also developed a National Statement on Ethical Conduct in Research Involving Humans (1999) which it is currently reviewing.

**What submissions say - issues**

**Complexity of privacy regime**

Submissions, including the Australian Department of Health and Ageing (99), the National Health and Medical Research Council (NHMRC) (32), the Australian Academy of Science (119) and University of Adelaide (28) point to the complexity of the privacy regime in Australia including both within the Privacy Act and between Commonwealth and state legislation and the impact this is having on health and medical research. They say, for example, that the co-existence of the NHMRC’s section 95 (public sector) and section 95A (private sector) guidelines and the interaction between the IPPs and the NPPs has created some confusion for researchers and consumers. Also they say that interpretation and implementation of Commonwealth and state privacy legislation is compromising individually and publicly beneficial research and health care. Problems include that private sector organisations are making incorrect decisions and adopting a highly conservative approach to privacy compliance\textsuperscript{182}. The NHMRC (32) says:

\begin{footnotesize}
\footnotesuperscript{180} The NHMRC also develops guidelines, similar to the section 95A guidelines, for research involving personal information held by the Australian Government Agencies under section 95 of the Privacy Act, which the Privacy Commissioner approves.
\footnotesuperscript{181} See sections 95A(1)-(4).
\footnotesuperscript{182} See for example, NHMRC 32, and also Professor Mark Israel, *Ethics and the Governance of Criminological Research in Australia*, NSW Bureau of Crime Statistics and Research, December 2004.
\end{footnotesize}
‘There is evidence that legitimate and ethical activities (which in some cases are vital to the quality provision of health care or the conduct of important health and medical research) are being delayed or proscribed because some key decision-making bodies are unable to determine, with sufficient confidence, whether specific collections, uses and/or disclosures of information accord with legislative requirements. The adoption of a highly conservative approach is resulting in excessive administrative effort and a reluctance to approve the legitimate use and disclosure of health information for the purposes of health care, as well as health and medical research.’

The Australian Nursing Federation (127) says that collection of data for health data registries, including the national asbestosis registry, is being impeded by individual organisations’ interpretation of the Privacy Act.

On the issue of the interaction between section 95 and section 95A guidelines, the NHMRC (32) says:

‘In particular, the differing requirements of Sections 95 and 95A are inconsistent and confusing. Their application to similar projects in different settings can result in different outcomes, without any apparent policy rationale’.

Inconsistencies between the two sets of guidelines include that while section 95 guidelines apply to proposals by an agency to collect use and disclose for ‘medical research’, the section 95A guidelines which apply to private sector organisations, refer to:

- proposals by and organisation for the collection, use and disclosure of health information for the purposes of research or the compilation or analysis of statistics, relevant to public health or public safety and
- proposals for collection by an organisation of health information for the purposes of management, funding or monitoring of a health service.

The NHMRC (32) says that there is no obvious rationale for these differences to exclude non-medical research by agencies from consideration under section 95 guidelines and medical research that is not relevant to public health or public safety from consideration under the section 95A guidelines.

The Department of Health WA (101) raises another inconsistency in relation to quality assurance and audit activities. It says that NPP 10.3(a) (iii) provides for collection, but not disclosure for management, funding or monitoring activities and that it should allow for disclosure for this purpose as well.

University of Adelaide (28) comments on the need to involve up to 10 national, state and other ethics research committees in national research proposals.
When consent needed

The NHMRC (32) points to the inconsistency between the NHMRC National Statement on Ethical Conduct of Research Involving Humans and the Privacy Act (the Statement), particularly in relation to when it might be appropriate to dispense with consent. The NPPs appear to be narrower in that they confine the circumstances in which consent can be dispensed with to when it is ‘impractical’ to obtain it. The Statement permits epidemiological research in broader circumstances, including where getting consent would cause ‘unnecessary anxiety’ or where the scientific value of the research would be prejudiced.

A number of other submissions also say that the circumstances where consent can be dispensed with are too narrow.183

Gaps and problems within NPPs

Slow up research

A number of submissions, for example, University of Adelaide (28) and the Australian Psychological Society (103) say that the private sector provisions have made the process of undertaking research more difficult. They say that they slow down the approval process and have an impact on gaining access to, and collecting, data.

General research

The AMA (29) and the South Australian Department of Health (95) point to the need to broaden the kind of research the NPPs cover. For example, the South Australian Department of Health says the NPPs do not cover non-health information. As a consequence, the Australian Compliance Institute (16) says that research that can have considerable public benefit has been hampered by the Privacy Act. It says that, on the basis that it may be possible to re-identify consumption data, organisations cannot provide this information (to universities, or government agencies, for example) without an individual’s consent.

Data linkage and registries

The South Australian Department of Health (95) and the Department of Health Western Australia (101) say that the NPPs do not seem to provide for data linkage and there is a need revamp NPP 10 to provide for this. Issues they raise include that the NPPs do not explicitly allow for flow of information for the development of Australia’s National Minimum Data Sets. The Department of Health Western Australia (101) says that while the information for these is nominally de-identified it does include date of birth, sex and postcode.

183 Australian Compliance Institute 16; University of Adelaide 28; Australian Epidemiological Association 30.
The NHMRC (32) is concerned that the Privacy Act directly impairs the establishment of registries. It says that use or disclosure of health information for this purpose is unlikely to be a directly related secondary purpose within the reasonable expectations of individuals under NPP 2 and so would appear to require approval by a HREC. However, the NHMRC (32) considers that such activities may be regarded as preliminary to research, rather than actual research, for the purposes of the NPP 2 exceptions to the need to get consent.

On the question of data linkage, the NHMRC (32) reports that some researchers have advised it that some HRECs appear to have discounted completely the potential to conduct research projects involving data linkage of health information without consent, and have rejected such applications out of hand, apparently in the ‘mistaken belief that such linkage is not ethically or legally acceptable’. It cites research it carried out which indicates that there was considerable support among the general public (66%) and health consumers (64%) for approved researchers to match information from different databases.

Likewise, it reports that there was an even higher level of support for approved researchers to access health information from databases where records are identified by a unique number rather than a name (general public 82%; health consumers 86%). It says its research also showed that nearly all health providers, data custodians, HREC members, and peak body representatives who participated in their stakeholder surveys acknowledged the importance of data linkage in improving effectiveness of treatment and consequently of public health.

On the other hand, in some stakeholder forums, it was said that many people do not know that their health information is, or might be, used for research without their consent, or understand the value of such research.

Complexity of reporting obligations

Submissions say, for example, the University of Western Australia Human Research Ethics Committee (1) and NHMRC (32), that the reporting obligations under the section 95A Guidelines are onerous and detailed. In particular they are concerned that the requirement to list the NPPs and the sub-sections referred to in reaching decisions is difficult to complete.

HREC decision making

An epidemiologist from the University of Adelaide (28) is concerned that what is in the public interest is being resolved by ethics committees who do not necessarily determine this issue on the basis of ethics considerations. The Australasian Epidemiology Association (30) is concerned about decision making on what is in the public interest being subject to opinions of individuals on HRECs. For example, it says that legal liability may override ethical or public interest matters in an ethics committee’s decision about whether on not
to approve a research proposal that involves collection, use or disclosure of personal medical information without consent.

University of Adelaide (28) considers that the current approach to community representation on HRECS may not be appropriate. Other submissions, for example, the South Australian Department of Health (95), says there are inconsistencies in the way HRECS are weighing up the benefit of a research proposal versus the threat to individual privacy.

De-identification and medical research

The Australian Consumers Association (15) says that the whole issue of de-identified data needs to be re-examined. The Australian Institute of Health and Welfare (100) also points to problems with determining what is de-identified data, and, says there is a need for more guidance. The Australian Consumers Association (15) is concerned that:

> 'as soon as something is deemed to be de-identified it no longer falls under the Privacy Act or the NPPs, but there is a vagueness surrounding the term... Indeed it seems that once a record is defined as ‘de-identified’ it is open slather, there is no need for consumer consent of ethics committee approval even though we have no good working definition of what de-identification means'.

The NHMRC (32) also says that stakeholders are experiencing difficulty in determining whether a person’s identity is ‘apparent or can be reasonably ascertained’. The Australian Nursing Federation (127) agrees that greater clarity is needed around the de-identification of electronic data and the point at which it is de-identified as well as the definition of de-identification itself.

There are mixed views among submissions about what people think about use of de-identified health information by third parties. The Australian Consumers' Association (15) says that when people go to the doctor, they are giving information on the basis that it will be used only in their clinical care. They do not expect that third parties will be trawling through their health records; even if it is in de-identified form. It says that in this sense third party access to data without the consumers’ knowledge is something of a breach of trust.

On the other hand, the Australian Department of Health and Ageing (99) says that consumers have very definite opinions about health information. On the basis of research it has carried out it says that consumers express strong reservations about identified personal information being made available for purposes other than their own clinical care on the one hand, but are generally very accepting of the notion of sharing de-identified personal health information amongst health planners and researchers.\(^{184}\)

What submissions say - addressing the issues

Consistency within the Privacy Act

The NHMRC (32) suggests combining the IPPs and NPPs into a single set of National Privacy Principles that apply to all relevant public sector and private sector agencies. It also recommends having a single set of research guidelines that apply to the collection, use and disclosure of health information without consent to apply to all health and medical research to which the Privacy Act applies. It says consistency could also be achieved by making the definition of ‘research’ consistent across all provisions of the Privacy Act and encompassing all health and medical research. The Australian Academy of Science (119) supports these kinds of measures.

National consistency

A number of submissions say that a single, simplified, national health privacy regulatory regime to replace, rather than supplement, the existing regulation should be pursued185. University of Adelaide (28) and the Australian Epidemiological Association (30) suggest that the states could refer matters to the Commonwealth.

Broadening research provisions to non-medical research

The Australian Compliance Institute (16) says that the Privacy Commissioner should agree to the need to expand the research category to meet government, environmental and community benefits. The Commissioner should have powers to exempt Privacy Act provisions and principles based on set criteria for research projects where there is government, community or environmental benefits.

Broadening circumstances in which consent not needed

The AMA (29) suggests that all medical research should be regarded as relevant to ‘public health and public safety’. Further, it suggests that there should be a broader construction of what is ‘public health and public safety’.

Submissions also suggest a number of ways that the provisions providing for when consent is not needed could be broadened. The AMA (29) says that the exemption from the need to get consent for collection or disclosure of health information for research purposes should be extended from when it is ‘impracticable’ to include when it is so inconvenient or unprofitable that the research would be hindered.

185 University of Adelaide 28; Australian Epidemiological Association 30; NHMRC 32.
The NHMRC (32) says that the NPPs should be brought into line with its Standards to include to allow consent to be dispensed with where it would cause ‘unnecessary anxiety’ or where the scientific value of the research would be prejudiced. However, in line with contemporary legal approaches to the concept of therapeutic privilege, it says the concept should be further defined to only encompass circumstances in which the procedures necessary to gain consent ‘are likely to seriously and adversely affect the well being (which includes the psychological health) of the person from whom consent would be sought’.

University of Adelaide (28) suggests that consent might be dispensed with in cases where inclusion in the research causes no physical or psychological harm to the individual. The Australian Epidemiological Association (30) says that most people think that consent should not be needed for access to ‘medical records for non-commercial medical research that has no effect on the individuals being studied and has been approved by an accredited research ethics committee’.

The Australian Compliance Institute (16) suggests that as for health and medical research, there should be special provisions to allow organisations to disclose personal information for research that will benefit government, environment and the community. Further, it says that the Privacy Commissioner should develop criteria for exempting, and have the power to exempt, such research from the Privacy Act.

Further work to clarify when consent is needed

Australian Consumers’ Association (15) recommends that the Office do further work on the sort of data-usage that requires consumer consent or ethics committee approval in the public and private spheres. It also says that the Office should do further work on the challenges involved in protecting consumer privacy in the face of numerous databases that could be used to re-identify records.

Ensure NPPs allow data linkage

A number of submissions suggest that the NPPs need to be either clarified or revamped to ensure that the great public benefit that can achieved from data linkage and data registries can be achieved. The Department of Health Western Australia (101) says that NPP 10.4 needs to be revamped as it does not permit the approach to data linkage in Western Australia, which allows a data custodian to retain data in identifiable form to enable the custodian to check the data. The Telethon Institute for Child Health Research (55) says that it is important that the privacy legislation understands the public good which results from the epidemiological analysis of existing data collected on the population which has been linked together.
Clarity meaning of de-identification

The NHMRC (32) recommends that the Office clarifies the meaning of ‘de-identified’, to make it clearer what information is and is not subject to the Privacy Act and ethics approval processes. The Australian Consumers’ Association (15) says that the Office should provide guidelines that set out a clear working definition of ‘de-identified’ data.

Simplify HREC approval process

A number of submissions agree that the procedure for gaining ethics approval to undertake linkage or record assessment research should be straightforward and streamlined186.

HREC reporting requirements

Submissions, including a Human Research Ethics Committee (1), the NHMRC (32) and the Australian Academy of Science (119) support measures to streamline the reporting requirements of Health Research Ethics Committees.

Legal protection for HRECS

University of Adelaide (28) and the Australian Epidemiological Association (30) say the law should be changed to protect ethics committees when they make reasonable decisions.

Raising awareness and acceptance

Submissions suggest a number of measures to increase public awareness and acceptance of use of health information for research, and in particular epidemiological research. These include the careful publishing of research findings and public health outcomes in the popular media and holding forums that highlight the need for this kind of research187. In some of the stakeholder forums it was said that there should be public debate and raising of community awareness on the issue of use of health information without individual consent.

The Health Consumers’ Council, Perth188 says there needs to be greater regard for consent when health information is used for research, or at a minimum there should be notice of what information is being collected and how it is to be used and/or disclosed and whether the use, disclosure or collection is required or authorised by or under law.

---

186 University of Western Australia Health Ethics Research Committee 1; University of Adelaide 28; Australian Epidemiological Association 30.
187 Australian Epidemiological Association 30, Telethon Institute for Child Health Research 55, NHMRC 32.
188 At a meeting in Perth, 12 November 2004.
Options for reform

Consistency in approach to research between private sector and Commonwealth public sector

It has been recommended (see recommendation 1) that there be a wider review of the Privacy Act. This wider review could include how to make the IPPs and the NPPs consistent. This would include considering the question of what guidelines were needed. The same guidelines could apply to the same kind of research, regardless of whether it involves private sector or public sector. However, the wider review would need to consider whether separate guidelines might be needed for non-medical research that does not involve health information. It could also include reaching a definition of ‘research’ that applies across both sectors.

Broaden NPPs to include research on humans, not just medical research

For non-health information this would involve amending NPP 2 which currently only has provision to allow for disclosure of health information for specified research purposes without consent. To ensure there is appropriate protection, there would need to be a process that would include a HREC approval process appropriate to non-medical research.

A possible reference is the Information Privacy Principles 10(f) and 11(h) of the Privacy Act 1993 (NZ), which allow personal information to be used or disclosed if the agency believes on reasonable grounds that the information is to be used for statistical or research purposes and will not be published in a form that could reasonably be expected to identify the individual concerned. This principle currently applies un-modified to non-health information. However, New Zealand has a health information privacy code which regulates the handling of health information, including for research purposes189.

It may not necessarily be appropriate to adopt the New Zealand approach to research involving non-health information without examining further whether the environment has changed sufficiently (for example, the increased ability to link data) to require a more strict approach, such as requiring there to be a HREC approach for research involving non-health information.

Nationally consistency in approach to protecting privacy in research, including health and medical research

This report has made recommendations in Chapter 1 on how greater national consistency could be pursued. Having a national health privacy code which includes provisions for research could be of help in this respect. There would have to be consideration of how the IPPs fit into this scheme. However, this

189 Health Information Privacy Code 1994 (NZ).
would not help to achieve consistency in the case of research that does not involve health information.

Clarify disclosure for the purpose of the management, funding or monitoring of a health service without consent

This could be done by:

- amending NPP 2.1(d) to include that organisations can disclose information for the purpose of the management, funding or monitoring of a health service without consent. (This would require them to go through a section 95A process.)
- adding an additional exception to NPP 2.1 that allows organisations to disclose information for the purpose of the management, funding or monitoring of a health service without consent. (This means they can do it without having to go through the section 95A process.)
- conducting an education campaign with HRECS and other key bodies, and private sector organisations generally, to ensure that they know that the Office’s guidelines say that disclosure for management, funding and monitoring is related to the primary purpose of collection and within people’s reasonable expectations and so does not require consent.

Inquiry into use of personal information for research

There could be an inquiry to determine with appropriate consultation and public debate:

- the appropriate balance between facilitating research for public benefit and individual privacy and right of consent
- whether special protections are needed for research for commercial purposes
- the privacy protections necessary if the balance is shifted towards data linking and more access without consent
- what public education is needed to ensure the community is aware of the uses made of their personal information and the protections in place to protect it when it is collected without consent

There is considerable evidence that key researchers, especially epidemiological researchers, consider that the current balance between privacy and the public benefit of research is too heavily weighted in favour of individual privacy to the detriment of research. By gaining access to population data and data linkage, the research might considerably benefit disadvantaged groups that are currently under researched.

There is evidence that taking an opt-in approach to participation in research significantly reduces the participation rate and therefore the scientific integrity
of research. In a study conducted by the University of Sydney\textsuperscript{190}, it was found that:

‘opt-in requirements significantly reduce the proportion of people ultimately recruited into a trial compared with an opt-out approach that was once commonplace. It has also shown that by increasing the number of eligible people approached to opt-in, a demographically similar study sample can be obtained. Furthermore, a study sample recruited by opt-in is more likely to include active, preventative health-seeking participants and those with a personal motivation such as a higher risk’.

The Office has received many submissions from researchers on this issue but few comments or submissions from a consumer point of view. Consumer research on this issue is mixed. Research conducted by the Office shows that individuals are concerned about their personal information being used, even in a de-identified form, for research purposes. Almost two thirds (64%) of respondents felt that an individual’s permission should be obtained before de-identified information derived from personal information about them is used for research purposes. One third (33%) of respondents felt that permission was not necessary.

On the other hand, the Australian Department of Health and Ageing research suggests that although consumers express strong reservations about identified personal information being made available for purposes other than their own clinical care on the one hand, they are generally very accepting of the notion of sharing de-identified personal health information amongst health planners and researchers.\textsuperscript{191}

This is a complex issue that goes beyond the remit of this Office. Getting this balance right will be important and should be resolved if initiatives to connect electronically health information are to succeed with community support.

Guidelines that clarify what is and is not de-identified personal information

As part of a wider inquiry into the Privacy Act, the issue of what is or is not de-identification could be considered. This is an important threshold issue which determines whether or not information is protected. Developments in technology have made it increasingly difficult to determine whether information is de-identified or not. In the meantime, the Office could provide guidance on this, which would help HRECs and researchers in their decision making.

\textsuperscript{190} Lyndal Trevena, Les Irwig, Alexandra Barratt, ‘The Impact of Privacy Legislation on the Number and Characteristics of People who are Recruited for Research: a randomised control trial’; in press.

\textsuperscript{191} It cites Research Report 5: What will be necessary to manage privacy, AC Neilson Consult, DoHA, 2003 p 16; Consumer Attitudes Towards Consent, Electronic Health Records and the Use of Health Data for Research Purposes, TQA Market Research report. October 2004, DHA.
Simplify reporting requirements for HRECs

This would involve the Office working with the NHMRC to reach a simpler format for reporting which better reflect the way HRECs make decisions in deciding whether or not to approve a research project. It would help to streamline the HREC process. However, there should still be an adequate level of accountability.

### 7.4 Recommendations: Research

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>60</td>
<td>As part of a broader inquiry into the Privacy Act (see recommendation 1), the Australian Government should consider:</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• how to achieve greater consistency in regulating research activities under the Privacy Act</td>
</tr>
<tr>
<td></td>
<td>• whether regulatory reform is needed to address the issue of de-identification in the context of research and the handling of health information</td>
</tr>
<tr>
<td></td>
<td>• where the balance lies between the public interest in comprehensive research that provides overall benefits to the community, and the public interest in protecting individuals’ privacy (including individuals having choices about the use of their information for such research purposes)</td>
</tr>
<tr>
<td></td>
<td>• whether there is a need to amend NPP 2 to permit the use and disclosure of personal information for research that does not involve health information</td>
</tr>
<tr>
<td></td>
<td>• undertaking further research and education work with the broader community to ensure that the balance between research and privacy accords with what the community expects and understands.</td>
</tr>
<tr>
<td>61</td>
<td>The Office will issue guidance in relation to NPP 2 to clarify that organisations can disclose health information for the management, funding and monitoring of a health service.</td>
</tr>
<tr>
<td>62</td>
<td>The Office will work with the National Health and Medical Research Council to simplify the reporting process for human research ethics committees under the section 95A guidelines.</td>
</tr>
</tbody>
</table>
7.5 Decision-making where capacity is impaired

Introduction

Impaired capacity and substituted decision-making

In order for an individual to give valid consent to privacy or other matters they must have the capacity to make an informed decision. Decision-making capacity can be impaired permanently or temporarily for a number of people for a range of reasons. These include cognitive disabilities such as acquired brain injury, dementia or mental illness. A child may lack capacity for legal or other reasons.

Role of carers

For adults with a decision-making disability, the role of substituted decision-maker may be entrusted to a spouse, carer, family member or friend. This can occur informally where the person with a decision-making disability is assisted by someone in their day-to-day affairs, or it can occur formally, for example where there is an order made under state or territory guardianship or administration legislation. Generally, formal guardianship and administration orders are made as a last resort only. Instead, there is a preference for informal arrangements 'where a family member, carer or friend serves as substituted or assisted decision-maker and often as primary advocate'. The spouse, carer, family member or friend conducts business, such as banking, dealing with utilities and welfare agencies, informally on the person’s behalf.

For children, generally the child’s parents have responsibility for decision-making on their behalf.

Problems for substituted decision-makers

In 2003-2004, members of the Australian Guardianship and Administration Committee (AGAC) wrote to the Office about privacy laws and difficulties carers were experiencing in conducting business on behalf of persons with decision-making disabilities. Submissions to the Review and comments made at stakeholder forums reiterated this issue.

---

192 Each Australian state and territory has its own protective guardianship and administration legislation with tribunals and agencies having the necessary powers to achieve the legislation's goals. Representatives from each jurisdiction comprise the Australian Guardianship and Administration Committee (AGAC). Its aim is to develop and promote interjurisdictional linkages. More information about AGAC and the guardianship and administration regimes of each jurisdiction is available at [http://www.ijcga.gov.au/](http://www.ijcga.gov.au/).

193 Australian Guardianship and Administration Committee 114.
Relevant privacy principles

Section 6 of the Privacy Act and National Privacy Principles (NPP) 2, 6 and 10 are relevant in this context.

Collection of sensitive information

‘Sensitive information’ is defined by section 6 of the Act and includes, amongst other things, an individual’s health information. Except in certain circumstances, an organisation cannot collect an individual’s sensitive information without their consent (NPP10.1).

One of those circumstances is where the collection of sensitive information is necessary to prevent or lessen a serious and imminent threat to the life or health of any individual, and the information concerns a person with an impaired decision-making capacity. In such circumstances, their sensitive information can be collected by an organisation without consent (NPP10.1(c)).

Disclosures of personal information

NPP 2 establishes the general rule that personal information must only be used or disclosed for the primary purpose for which it was collected. However, there are exceptions to this general rule.

These exceptions enable organisations to make judgements about disclosing an individual’s personal information to a third party in certain circumstances. The consent of the individual, whether express or implied, is not the only exception to this general rule.

For example, where a guardianship or administration tribunal has made an order appointing someone to act on an individual’s behalf, the disclosure of relevant personal information about the individual by an organisation to the guardian or administrator would be ‘authorised by law’ in terms of NPP 2.1(g).\textsuperscript{194}

Disclosures of health information

Further exceptions to the general rule about disclosures are to be found in NPP 2.4, 2.5 and 2.6 regarding the ‘health information’ of persons with an impaired decision-making capacity. These provisions represent a scheme that facilitates, within certain limits, disclosures of health information to ‘responsible persons’ (as defined in NPP 2.5 and 2.6).

\textsuperscript{194} See OPC Guidelines on Privacy in the Private Health Sector at http://www.privacy.gov.au/publications/hg_01.html#b27
Discretion to disclose

The provisions of NPP 2.4, 2.5 and 2.6 are structured to give health service providers a discretion about disclosing the health information of an individual with impaired capacity when, broadly speaking, it is in the individual’s interest to do so. That discretion can be exercised by the health service provider in certain circumstances explained below (NPP 2.4(b)).

Where it is necessary for the care and treatment of the individual, or for compassionate reasons, a health service provider may disclose relevant health information about the individual to certain persons, providing that it is not contrary to the reasonably ascertainable wishes of the individual (NPP 2.4(c)). Such disclosure must be limited to what is necessary and reasonable to meets its purpose (NPP 2.4(d)).

If a disclosure is permitted by NPP 2.4, the Privacy Act does not guide the organisation in whether or not to provide information to carers, family members or other responsible persons. This is a matter for the organisation’s professional judgement in line with its own policies and other legal obligations in the circumstances of each case.

Access to personal information

NPP 6 gives individuals a general right of access to personal information about them held by private sector organisations, subject to certain exceptions.

If an individual with an impaired decision-making capacity has an appointed guardian or administrator, the latter may exercise the right of access under NPP 6 on the individual’s behalf. This is the case to the extent the guardian or administrator is appointed to stand for the individual under law. Access rights exercised by a guardian or administrator on behalf of an individual are subject to the same exceptions under NPP 6 as they are for any other person.

What submissions say - issues

Refusing services

Submissions express concern that government agencies, businesses (such as banks and utilities) and other service providers may be causing hardship to individuals, who are dependent on substituted decision-makers, by adopting unduly cautious interpretations of privacy legislation. These concerns were also raised in stakeholder forums. The AGAC submission (114) refers to the following examples:
• Utilities have refused to accept directions about the supply of services to the home of an elderly woman with dementia from members of her family. The companies gave privacy laws as the reasons for their refusal.

• In the absence of express authorisation by a policy holder with physical and intellectual disabilities, an insurance company refused to disclose information about the client’s policy to the policy holder’s parents who cared for them and assisted in their insurance arrangements.

• Both an Australian Government welfare agency and a bank refused to disclose financial information to the carer of a client with a mental illness. The information was denied ‘on the grounds of privacy’.

### Implementing privacy laws

Submissions refer to businesses requiring the production of an express authorisation from individuals (with impaired decision-making capacity) so that their carers can transact business on their behalf. Other service providers ask for some formal evidence of authority to permit a carer to act on the individual’s behalf, such as an order from a tribunal:

> ‘In all facets of daily life…, I am constantly challenged as not being the person to conduct business on behalf of (my son)’ - the mother of a man with an intellectual disability (AGAC 114).

The issue of cost is also raised in a submission from a father of a dependent adult child:

> ‘Most of these people insist on a power of attorney addressed to them which now costs over $100.00 to organise’ (7).

Submissions also support the view that front-line staff of service providers may be implementing a ‘low-risk’ or narrow approach to privacy laws. The Private Health Insurance Ombudsman (10) notes difficulties that parents had experienced in obtaining information about disabled adult children in their care. These difficulties, the submission also noted, were increasingly being resolved by putting appropriate administrative arrangements in place.

### Consistent privacy standards

Submissions suggest that consistency between the privacy principles operating in the federal public sector and the private sector would assist the work of carers for people with decision-making disabilities.

> ‘Each sector should have the same privacy standard, set at the level of the NPPs’ (AGAC 114).
Do the NPPs work for those with decision-making disabilities?

A lack of decision-making capacity should not mean that individuals miss out on obtaining access to services; neither should their privacy rights be undermined because they cannot make their own decisions.

Submissions support the view that the protection of an individual’s privacy rights under the NPPs is not incompatible with their reasonable enjoyment of services. The understanding, interpretation and the application of the NPPs by agencies, businesses and service providers are identified in submissions as needing improvement.

Options for reform

Amend NPP 2 to permit disclosures of non-health information without consent where decision making disability

There appears to be some significant concern that NPP 2 does not readily permit the disclosure of certain personal information about an individual with a decision-making disability where this may be manifestly in their interests.

The Office is aware of concerns about the Privacy Act potentially limiting or denying the ability of some private organisations (such as utilities or financial institutions) to disclose non-health information about a person to a carer, family member or friend where this might be necessary to manage the person's affairs. This information may be personal or financial details relating to the provision of a utility or service (for example water, gas, electricity or telephone), or another key element of their affairs (for example, financial affairs).

It may be appropriate to amend NPP 2 to include a provision like NPP 2.4, which would permit the disclosure of non-health information to certain people (such as those listed in NPP 2.5) in limited circumstances. Care will be needed to avoid creating too broad a permission to disclose and thereby putting at risk the financial and other interests of the person with a decision-making disability. Of course, an amendment to NPP 2 in this manner would always leave the discretion to disclose with the organisation, which would need to satisfy itself that the disclosure was warranted and necessary to secure or safeguard the interests of the individual.

The Office would need to issue guidance on the application of such provisions should they be inserted into the Privacy Act.

Binding guidelines on NPP 2 and decision making disability

Rather than amend NPP 2 by adding a further general exception, the Privacy Act could be amended to provide for a power to issue binding guidelines.
about the handling of personal information in certain circumstances. The power to make binding guidelines is discussed in section 5.6.

The binding guidelines could amend NPP 2 to allow for the use and/or disclosure of personal information in circumstances relating to decision making disability set out in the guidelines. To ensure adequate transparency and scrutiny, such guidelines could be legislative instruments for the purposes of the *Legislative Instruments Act 2003*.

**Public Interest Determination to vary NPP 2**

Rather than amend NPP 2 by adding a further general exception, the Privacy Commissioner could make a public interest determination (under Part VI of the Privacy Act) to permit disclosures of personal information relating to a person with a decision-making disability in certain circumstances.

Given the ongoing nature of the information-handling under consideration, the non-permanent natures of such determinations may not be the most appropriate regulatory solution to this issue. To provide the assurance and stability in the law that these issues call for, it may be more appropriate to resolve the matter with a longer-term regulatory option.

**No change**

As submissions and input to the stakeholder forums did not call specifically for changes to the Privacy Act, it may be argued that it is appropriate not to amend the legislation in this area. If this were the case, then the emphasis would appear to rest on awareness and education.

**Education and awareness**

There was greater agreement among stakeholders that better understanding of how the NPPs work in this area is important. More practical guidance from the Office on the permissible information-handling acts and practices of agencies and organisations may remove many of the difficulties experienced by individuals with decision-making disabilities and their carers.

In its submission, AGAC (114) referred to the *Best Practice Guide: Privacy and people with decision-making disabilities*, published by the Office of the NSW Privacy Commissioner, as an example of a resource that might assist in educating and raising awareness around these issues\(^{195}\).

The Office could consult with the NSW Privacy Commissioner and carefully consider these guidelines with a view to adopting, with agreement, the guidance material that correlates with the NPPs. The Office could work with stakeholders to further develop this guidance to deal with other issues. The resulting materials could be used nationally to minimise the difficulties currently experienced by people with decision-making disabilities, their carers and the organisations with which they deal. Such work would be subject to the Office being provided with sufficient resources.

7.6 Recommendations: Decision-making where capacity is impaired

63 The Australian Government should consider, in order to ensure that the Privacy Act does not prevent individuals with a decision-making disability from receiving a range of utilities and other services, amending NPP 2 to permit the disclosure of non-health information to a class of persons the same, or similar, to that described in NPP 2.5, where an organisation considers the disclosure to be necessary for the management of the person’s affairs in a way that their financial or other interests are secured or safeguarded. It would be appropriate to consider developing such an amendment in consultation with the Australian Guardianship and Administration Committee.

64 The Office will, in recognition that disclosures of health information under NPP 2 are appropriately permitted in law but may not occur in practice, develop further and more practical guidance.

7.7 Law enforcement

Law and policy

Protecting the community and privacy

The community has an interest in its security and safety being protected by government regulatory bodies and law enforcement agencies. In the course of carrying out their activities and functions, enforcement bodies, government agencies and regulatory authorities collect personal information from a range of sources, including private sector organisations. The Privacy Act seeks to balance the public interest in effective law enforcement with the protection of individuals’ privacy.

The Privacy Act permits organisations to lawfully co-operate with agencies performing law enforcement functions. The Act is not intended to hinder organisations’ involvement and co-operation with law enforcement bodies.
The Act is not intended to interfere with other legal obligations (for example, common law duties) that organisations might have and which affect the use and disclosure of personal information.

**Relevant privacy principles**

Section 6 of the Act and NPPs 1, 2, 6 and 10 are relevant in this context.

**Collection of sensitive information**

’Sensitive information’ is defined by section 6 of the Act and includes an individual’s health information and criminal record. Except in certain circumstances, an organisation cannot collect an individual’s health information without their consent (NPP10.1).

One of those circumstances is where the collection is required by law under NPP 10.1(b). Health service providers, for example, are required by state and territory public health legislation, to collect health information about individuals with certain notifiable diseases. Similarly, under child protection legislation, private sector educational institutions must check the criminal record histories of their employees.

**Disclosure to law enforcement bodies**

NPP 2 establishes the general rule that personal information must only be used or disclosed for the primary purpose for which it was collected. There are exceptions to this general rule, including permitting an organisation to use or disclose personal information for law enforcement and regulatory purposes. These exceptions are set out in NPP 2.1 (f), (g) and (h).

Generally described, these exceptions permit an organisation to use or disclose personal information in situations such as where:

- The organisation has reason to suspect that unlawful activity is occurring (or that it has occurred or may occur), and it must use or disclose the personal information in its own investigation of the matter, or to report the matter to a relevant person or authority (NPP 2.1(f)).

- The use or disclosure is required or authorised by or under law (NPP 2.1(g)).

- The organisation reasonably believes the personal information is needed for use or disclosure by (or by another on behalf of) a law enforcement body for such things as the prevention, detection, investigation and similar activities relating to the criminal law and laws that impose a penalty or sanction; for the enforcement of laws relating to the confiscation of the proceeds of crime; to protect the public revenue; to prevent, investigate
and take other steps in relation to seriously improper conduct; or in the preparation for, or conduct of, court and tribunal proceedings (NPP 2.1(h)).

Section 6 of the Act defines ‘enforcement body’ to include such agencies as the Australian Federal Police, state and territory police services, as well as regulatory bodies such as the Australian Securities and Investments Commission.

**Discretion to disclose**

An organisation has discretion regarding whether or not to disclose personal information to a law enforcement body; that is, unless there is another law that requires the disclosure. If a disclosure is permitted by NPP 2, but not required by another law, the Privacy Act does not tell the organisation whether or not to provide personal information to a law enforcement body. The organisation must make its own judgement considering its own policies and any other obligations in the circumstances of each case.

**Access and law enforcement**

NPP 6 gives individuals a general right of access to personal information that an organisation holds about them. In certain circumstances an organisation can withhold access; these circumstances are set out in the exceptions to NPP 6. They include exceptions to access for law enforcement or regulatory purposes; for example, NPP 6.1(j) permits an organisation to deny access to an individual when this would prejudice activities being carried out by, or on behalf of, an enforcement body.

**Issues paper**

The issues paper asked if the right balance has been struck between privacy and the public interest in effective law enforcement. It asked how the relevant NPPs are working in a law enforcement setting and whether steps are needed to redress any imbalances between these competing interests.

**What submissions say - issues**

**Law enforcement bodies**

Representatives of law enforcement officers said that some organisations have declined to provide personal information that was reasonably necessary for their enquiries, giving privacy legislation as the reason for their refusal. The Police Association of Victoria (116) states:

‘Our members are being denied access to information by some areas of the Private Sector Community on the basis that the information is protected under the Privacy Act’.
Office of the Privacy Commissioner

The Australian Federal Police (AFP) (129) notes the reluctance of some organisations to provide personal information in some circumstances. This can occur for a range of reasons including a lack of understanding on the part of the organisation about how the National Privacy Principles operate (that is, that they are permitted to disclose personal information for law enforcement purposes), concerns about disclosures being detrimental to commercial or other business outcomes, the costs of complying with a request for information, or concerns about litigation by those to whom the information relates.

Greater awareness and education is recognised as going some way toward resolving organisations’ concerns in this area. However, other solutions outside the Privacy Act may be needed. For example, the AFP mentions powers such as being able to issue a ‘notice to produce’, which could compel (or more clearly authorise) disclosure of certain information by an organisation.

**Private sector organisations**

On the other hand, pharmacists indicate that in some circumstances ethical obligations of confidentiality prevent them from disclosing personal information about their clients to law enforcement officers. The Pharmacy Guild of Australia (93) says that, generally, law enforcement officers and the general community are unaware of pharmacists’ obligations of confidentiality. The Guild (93) submits:

> There is an underlying belief in the community that confidentiality between a pharmacist and patient is not as vital as it is for a doctor and patient.

**Consequences of lack of awareness**

Submissions state that a lack of awareness about privacy legislation and obligations of confidentiality had undesirable consequences. The Police Association of Victoria (116) refers to a ‘risk of undermining the core functions of our members through ‘misunderstandings’ about the Privacy Act.

The Pharmacy Guild of Australia (93) submits that refusing to provide information to police officers ‘can often be quite intimidating for a pharmacist’.

These submissions were backed up by comments at stakeholder consultations.

**Australian Institute of Private Detectives**

The Australian Institute of Private Detectives (38) suggests the definition of ‘enforcement body’ should be extended to include private detectives. This would permit private detectives to more readily collect personal information
about individuals from organisations. This matter is further explored at section 7.9.

**Enquiries from the private sector**

Since the introduction of the National Privacy Principles, the Office has received a significant number of enquiries from organisations about their obligations when asked to disclose data to law enforcement officers.

**Options for reform**

**No changes to the law**

Submissions do not call for changes to the NPPs in the law enforcement context. Generally, it appears the construction of the law is considered to be reasonable, but problems seem to arise in its application.

It seems appropriate, therefore, not to change the law, but to focus on how the law is understood and applied.

**Greater awareness and education**

If the law is considered to be appropriate, there is a need to consider whether greater awareness and education is necessary to develop a better understanding of how the NPPs are intended to work in the law enforcement context. This is a matter that has been demonstrated through the Review.

There appears to be a need for greater education on the circumstances of permissible disclosures of personal information by private sector organisations to law enforcement bodies under the NPPs.

The Office could work with the law enforcement sector and relevant industry bodies to develop more practical guidance about personal information handling and law enforcement in the context of the NPPs. This would help to make the Act work more effectively. For such work to be effective it would require additional resources for the Office.

**7.8 Recommendation: Law enforcement**

65 The Office will work with the law enforcement community, private sector bodies and community representatives to develop more practical guidance to assist private sector organisations to better understand their obligations under the Privacy Act in the context of law enforcement activities.
7.9 **Private investigation**

**Introduction**

The private sector provisions seek to balance an individual’s right to privacy with other social interests that compete with privacy. The Office has been made aware for some time now that those involved in private investigation consider that a number of social interests that their work furthers are being impeded by the private sector provisions of the Privacy Act. The private sector provisions make no specific provisions for the activities of private investigators.

**What submissions say - issues**

**Work of private investigators**

The Australian Institute of Private Detectives (AIPD) (38) comments extensively on how the Privacy Act impacts on their functioning. It outlines the work of private investigators as being crucial in workers’ compensation and third party injury cases as well as commercial areas, such as process serving and debt collection and the repossession of goods and/or services. It says private detectives sometimes play a watchdog role in conducting investigations into the conduct of the authorities on the behalf of individuals.

**Unequal access to information**

The main concern expressed by the AIPD (38) is that private investigators are excluded from the definition of ‘enforcement body’ in the Privacy Act. The AIPD is concerned that enforcement bodies have access to information under NPP 2.1 that is denied to other organisations and individuals. The AIPD submits that this inequality in access to information could lead to inequality and unfairness before the law.

The AIPD (38) refers extensively to legislation, Charters and Treaties from around the world in demonstrating that an individual has the right to have equality before the law and a right to a fair trial\(^{196}\). The AIPD uses these documents to substantiate its argument that private investigators should have the same right of access to information as enforcement bodies. The submission argues that the Privacy Act excludes private investigators and individuals from being able to access information in order to prepare adequately for matters or potential matters before a court or tribunal. The submission contends that because enforcement bodies can access this information, private investigators and other individuals are at a disadvantage before courts and tribunals and this means there is inequality before the law.

\(^{196}\) The United States Drivers Privacy Protection Act 1994; Europa Justice and Home Affairs Charter of Fundamental Rights; Human and Constitutional Rights South Africa; International Covenant on Civil and Political Rights; European Convention on Human Rights
The AIPD argues that, particularly in relation to criminal matters, if an individual does not have the right to access information to adequately defend themselves, that person has not been granted a fair trial.

The AIPD argues that equality before the law is a constitutional right. It argues that the inequality in access to information caused by the Privacy Act, resulting in inequality before courts and tribunals means the Privacy Act is unconstitutional. The AIPD launched legal proceedings in the Federal Court of Australia during March 2004 challenging the constitutional validity of the Privacy Act. The Application stated that:

‘the Privacy Act is unconstitutional due to section 6(1) as it denies the right to access information in the public and private sectors to private investigators acting on behalf of their clients for matters and potential matters before the courts and tribunals. It also denies ordinary citizens representing themselves the same rights to access information in the public and private sectors for matters and potential matters before the courts and tribunals’.

The AIPD later filed an amended Application claiming that the Office had declined to grant a Public Interest Determination under section 72(2) of the Act to authorise the disclosure of personal information by organisations to its members for the purpose of investigating matters in relation to litigation or potential litigation.

In November 2004 the case was dismissed on the grounds that the Court lacked jurisdiction to grant relief, and costs were awarded to the Commonwealth.

Do the private sector provisions unduly hamper the activities of private investigators?

Collection

One concern for private investigators could be the obligation to let individuals know if a private investigator is collecting information about them under NPP 1.3 and NPP 1.5. However, Information Sheet 18 ‘Taking Reasonable Steps to Make Individuals Aware that Personal Information about Them is Being Collected’, published by the Office, makes it clear that in some situations, many of which may apply to the work of private investigators, no steps will constitute reasonable steps to notify. For example, the information sheet says:

‘To investigate and confirm a suspicion of fraud or unlawful activity it will often be necessary to collect information about an individual’s activities without alerting them to the fact that information is being collected for this purpose. Raising awareness about this may give the

Reference is made to the decision in Leeth v The Commonwealth of Australia [1992] HCA 29
individual an opportunity to cover-up evidence of unlawful activity. There is a clear public interest in the detection of fraud and unlawful activity.

In the case of fraud investigation which is in the public interest, it will generally be reasonable not to take steps to ensure awareness of the NPP 1.3 matters at the time of collection, where:

- fraud or other unlawful activity is suspected on reasonable grounds
- information being collected is necessary for the investigation of the suspected fraud or other unlawful activity and
- there are sound reasons for concluding that providing notice at or before the time of collecting the information would significantly reduce the integrity and usefulness of the information.’

These circumstances arise where unlawful activity is being investigated. However, investigators may be investigating activity which is improper rather than unlawful; for example, misuse of employer resources, abuse of power or position, or marital infidelity. Complying with NPP 1.3 or NPP 1.5 in these circumstances may impinge on the activities of private investigators. However, it is considerably less clear in these circumstances that the public interest in investigating possibly improper activity outweighs the individual and the public interest in individuals being aware that they are under investigation.

**Disclosure**

The AIPD (38) submits that the activities of private investigators are severely hampered by NPP 2. Its main concern is that NPP 2 prohibits organisations from disclosing information to private investigators. The AIPD (38) argues that NPP 2 limits the ability of private investigators to have access to all information necessary to proceed before a court or tribunal. A similar argument is made by the Australian Collectors Association, Institute of Mercantile Agents, Australian Institute of Credit Management (Joint Credit Industry) (115) in relation to debt collection. Their submission argues that the Privacy Act impedes debt collection practice as credit providers are unable to access information about individuals that would enable them to investigate fraud or serve legal process.

The submission also raises concerns that the Privacy Act limits the ability of credit providers to access information that would assist in locating debtors who have left their last known addresses even where the defaulters have provided express authority.

It is possible that, without consent, NPP 2 will impede the ability of private investigators to collect information from organisations in these circumstances. The law enforcement exceptions to NPP 2, such as NPP (f) (g) and (h) do not apply to these situations.
Other legislation that impacts on private detectives

The AIPD (38) contends that the Privacy Act impacts on the ability of private detectives to access information needed to investigate fraud and other crime. However, there is other state and territory legislation and also privacy-related legislation at the federal level that also has an impact on the ability of private detectives to have access to information. For example, state legislation prevents information about drivers’ licences from being disclosed. The Commonwealth Electoral Act 1918 prevents private detectives from accessing the electoral roll, except in hard copy. Some states also have privacy legislation which may prevent government agencies from disclosing personal information to private detectives. As a result, this issue must be seen as broader than the Privacy Act.

Other views

The Australian Privacy Foundation (90) is concerned that the business activities of private detectives are significantly likely to be in violation of an individual’s privacy. In criticising the small business exemption, the Australian Privacy Foundation (90) remarks that ‘some of the most privacy intrusive activities are carried out by small companies [such as] private detectives’. The core business of private detectives appears to involve collecting information about individuals without their consent upon the wish of a third party client. There are public interest arguments in favour, therefore, of regulating the activities of private detectives.

Private detectives and other jurisdictions

The Data Protection Act 1998 (UK) enables the disclosure of personal information in order to establish, exercise or defend legal rights. Privacy provisions and practices in other jurisdictions do not appear to be significantly out of step with the private sector provisions.

United Kingdom

Subsection 35(2) of the Data Protection Act 1998 (UK) provides an exemption from the non-disclosure provisions where the disclosure is necessary:

(a) for the purpose of, or in connection with, any legal proceedings (including prospective legal proceedings) or

(b) for the purpose of obtaining legal advice, or is otherwise necessary for the purposes of establishing, exercising or defending legal rights.

New Zealand

Under the New Zealand Privacy Act 1993, Information Privacy Principles 2, 3, 10 and 11 provide an exception where the agency collecting or holding the
information believes on reasonable grounds that non-compliance is necessary:

‘to avoid prejudice to the maintenance of the law by any public sector agency, including the prevention, detection, investigation, prosecution, and punishment of offences’.

The exception refers only to ‘public sector agency’. Private investigators as private sector agencies would not, therefore, be able to rely on this exception. Discussion Paper No 8 states:

‘The words ‘public sector agency’ are included in the exception to ensure that only agencies with a proper function connected with the maintenance of the law would be able to act in reliance on the section. For instance there was concern that if the exception was not limited in this way that private investigators might rely on the exception to justify their actions’.198

Canada

*The Personal Information Protection and Electronic Documents (PIPED) Act* (2000, c. 5) does allow for information to be collected without consent where the knowledge or consent of the individual would compromise the availability or accuracy of the information, and where the collection is ‘reasonable for purposes related to investigating a breach of an agreement or a contravention of the laws of Canada or a province.’

The Canadian Privacy Commissioner expressed reservations, however, about granting an entire industry or industry body status as an investigative body, particularly because this power may be abused by companies. According to the Canadian Privacy Commissioner, private investigative work can be conducted without resorting to the provisions that allow for disclosures to designated investigative bodies without consent199. Instead, the Canadian Privacy Commissioner recommends that the Private investigator act as an ‘agent’ of the company. If the client organisation has the consent of the individual, this would then flow through to the investigator.

**Options for Reform**

**Amend definition of enforcement body under section 6(1)**

The AIPD considers that the way to even up the imbalance between the amount of information available to enforcement bodies (as defined in section 6(1)) on one side and private detectives on the other is to amend the Privacy Act to include private detectives in the definition of ‘enforcement body’. The

---

198 Discussion paper no 8 Law Enforcement Information and Other Related Issues.  
http://www.privacy.org.nz.html

199 http://www.privcom.gc.ca/speech/2003/02_05_a_030320_e.asp
definition of ‘enforcement body’ could be amended to include ‘private investigators in relation to matters before courts or tribunals’.

However, it is not clear that the public interest reasons for doing so outweigh the risks to the privacy of individuals. The fact that Parliament has found it in the interests of the community for law enforcement agencies to have access to information, does not necessarily mean that all others should have an equal right. Although some of the activities of private investigators may appear to be similar to those of law enforcement agencies, particularly where they are acting on behalf of law enforcement agencies, or are carrying out activities that might have been done by law enforcement agencies in the past for example, investigating fraud, this is not the case for all of their activities.

Private investigators carry out investigations on behalf of third parties, who are often private individuals. Law enforcement agencies carry out investigations on behalf of the state. Giving private investigators access to personal information in this way could mean that they are carrying out investigations without the important scrutiny and accountability mechanisms that law enforcement agencies are subject to.

Accountability

Private detectives licences are granted in New South Wales, Queensland, Victoria, South Australia and Western Australia under various pieces of legislation200. Such licences can be cancelled if a private detective’s conduct breaches legislation. Members of the AIPD must also comply with the association’s Code of Ethics. According to the Joint Credit Industry submission (115), almost all members of the Institute of Mercantile Agents hold a commercial agent licence and a private inquiry agent licence.

Nevertheless, the laws and institutional bodies that regulate private detectives are quite different to the conditions under which law enforcement agencies operate. For example, complaints against state or territory police forces that conduct surveillance operations and collect individual’s personal information can be made to the state or territory ombudsman or the police complaints commission.

Accountability mechanisms help to legitimise surveillance and reassure the community that the negative impacts on privacy by law enforcement activities are minimal and warranted. Accordingly, the Privacy Commissioner has suggested in submissions201 and a recent speech202 that new surveillance and law enforcement policies and initiatives that potentially violate privacy should be balanced by accountability measures that ensure collection and disclosure


of individual’s personal information is conducted with accountability and that collection is justified and proportional to the threat.

Private detectives can be distinguished from other enforcement bodies on the basis that they are not accountable to the government or the community, or any accountability body such as an ombudsman who can investigate complaints and award compensation, in the same way that law enforcement agencies are. It would therefore be difficult to recommend private detectives be accorded similar access rights to personal information as law enforcement agencies as proposed by the AIPD.

On the other hand, the AIPD and the Joint Credit Industry raise some issues relating to the public interest that may merit further consideration. There is a social interest in individuals being able to take effective action to recover debts owed to them, or to find a person who is at fault in a car accident. It is also fair that individuals be able to prepare a defence case for court proceedings. Where the balance lies however is not clear on the evidence so far available to the Office.

**Public Interest Determination**

The Privacy Commissioner could issue a Public Interest Determination enabling organisations to private detectives acting in specified circumstances. The PID process involves public consultation and could be a chance for stakeholders to provide views and information on where the balance in public interest lies. However, as discussed, the issues on access to personal information arise more broadly then the Privacy Act, and a PID would not necessarily solve all the matters of concern to private investigators. It is also the case that even if actions were taken to allow organisations to disclose personal information to private investigators without consent, it cannot force organisations to do so.

This is a complex matter. There are many social policy issues involved in this debate and the wider community should have the opportunity to comment on this issue. There are also a range of laws that have an impact on the activities of private investigators. This would be a matter for state and territory governments.

It would therefore be preferable for the governments to consider this issue so that there is a wider public debate with all relevant federal, state and territory stakeholders involved.

**Private detectives acting as agents**

For private investigators acting as agents of organisations such as insurance companies, it may be possible to gain consent to collect through the organisation. The notice given by an insurance company, for instance, could
flow through to cover the investigator\textsuperscript{203}. Insurance companies could make individuals aware of NPP 1.3 matters at the time a customer takes out an insurance policy, or at the time the customer makes a claim. The notice could include information about the general circumstances in which the insurer might engage a private investigation firm, the circumstances in which the customer could be subject to covert surveillance, what the information could be used for and to whom the information would be disclosed.

### 7.10 Recommendation: Private investigations

| 66 | The Australian Government, through the Attorney-General, should consider requesting that the Standing Committee of Attorneys General (SCAG) consider the issues raised by the Australian Institute of Private Detectives as they are broader than the Privacy Act. |

### 7.11 Alternative Dispute Resolution

**Alternative Dispute Resolution**

The National Alternative Dispute Resolution Council describes Alternative Dispute Resolution (ADR) as ‘processes, other than judicial determination, in which an impartial person (an ADR practitioner) assists those in a dispute to resolve the issues between them’. ADR schemes provide flexible and affordable redress to consumers and small businesses against particular industry sectors. ADR schemes operate under Commonwealth Benchmarks (1997 Benchmarks for Industry Based Customer Dispute Resolution Schemes), Australian Securities and Investments Commission (ASIC), Corporations Act 2001, Telecommunications Act 1997 and the Telecommunications (Consumer Protection and Service Standard) Act 1999.

**What submissions say - issues**

Five ADR schemes (56) comment on the impact of the private sector provisions on ADR in a joint submission to the Review\textsuperscript{204}. The schemes acknowledge the competing public interests of an individual’s rights to privacy and efficient and effective ADR schemes. The schemes argue that compliance with NPP 1 and NPP 2 may delay the processing of information largely because, unlike many organisations covered by the NPPs, ADR schemes are unable to determine in advance what information will be collected and therefore how it will be used or disclosed.

\textsuperscript{203} This is a preferred approach of the Canadian Privacy Commissioner.

\textsuperscript{204} Banking and Financial Services Ombudsman Limited (BFSO), Insurance Ombudsman Service Limited (IOS), Financial Industry Complaints Scheme Limited (FICS),
**Third Party Information**

Under NPP 1.5, where an organisation collects information about an individual from a third party, there is an obligation to take reasonable steps to inform the individual about the collection, use and disclosure of the information. Relying on advice from the Office that ‘reasonable steps to inform’ can include no steps, the ADR schemes do not generally inform individuals of its collection, as this would breach confidentiality obligations. The joint submission states that the guidance provided by the Office through its information sheets has been useful in interpreting the NPPs, and in particular NPP 1.3 and 1.5. The submission raises concerns that this advice does not provide legislative protection. The schemes raise concerns that this policy advice has not been tested in the courts and are not enforceable. This is discussed in Chapter 4.

**ADR schemes as self-regulatory agencies**

The Office has issued advice that self-regulatory agencies such as the Telecommunications Industry Ombudsman (TIO) and Banking and Financial Services Ombudsman (BFSO) are authorities to which an organisation may report unlawful activity under NPP 2.1(f). The joint ADR submission (56) is concerned that the Privacy Act provides no clear authority, however, for such information to be provided to or collected by ADR schemes in other circumstances, for example, when they handle personal information that is not connected to unlawful activity and would therefore appear to fall outside NPP 2.1(f).

They say further, that despite the advice given by the Office, organisations have refused to disclose information needed by ADR schemes to investigate a claim for fear that they would be in breach of the NPPs. The ADR schemes submit that the application of the NPPs to ADR schemes is uncertain and that this uncertainty has impacted on the schemes’ efficiency and potentially on their effectiveness.

**Sensitive Information**

The ADR schemes (56) submit that many disputes brought to ADR schemes are from or about people with mental or physical illnesses. This is of relevance as determinations and negotiated settlements often take into account health or other sensitive information about a disputant or other individual. While the submission notes that NPP 10.1(e) allows for collection of sensitive information where the collection is necessary for the establishment, exercise or defence of a legal or equitable claim, the ADR schemes contend that it is not always clear at the time of collection that this exception will apply.

---

205 Information Sheet 7 – Unlawful Activity and Law Enforcement.
What submissions say - addressing the issues

Amend NPPs 1, 2 and 10

The ADR schemes (56) suggest that NPPs 1, 2 and 10 be amended to include an express exemption for ADR schemes. The submission declares that this will have no greater effect than formalising the policy advice already provided by the Office.

The submission requests that ADR schemes be specifically exempt from the NPP 1 requirement to inform individuals of collection where to do so would prejudice an obligation of privacy owed to a party to the dispute. The submission also suggests amendment of NPP 2 to enable use by and disclosure to ADR schemes for the purpose of dispute resolution. Finally, the submission suggests NPP 10.1(e) be amended to include as permitted purposes, collection for the investigation and resolution of claims by ADR schemes.

Options for Reform

Amend NPPs

It appears that the NPPs may impact on the efficiency of ADR schemes. NPP 2 could be amended to enable use by and disclosure to ADR schemes for the purpose of dispute resolution. NPP 10.1(e) could also be amended to enable collection of sensitive information where it is necessary for the investigation and resolution of claims under ADR schemes. The Privacy Act would need to define what schemes this amendment would apply to.

Amend definition of ‘law enforcement agency’

By amending the definition of law enforcement agency to include ADR schemes, ADR schemes may be given more freedom under NPP 2 than they require to carry out their functions. As ADR schemes do not generally act as law enforcers, such an amendment would not appear to be appropriate.

Public Interest Determination

The Commissioner could make a Public Interest Determination under section 72 of the Privacy Act that would exempt ADR schemes from the full application of NPPs 1, 2 and 10. As the concerns reported by the ADR schemes are likely to be ongoing, amendment to the Privacy Act would provide greater clarity in the law.
7.12 **Recommendations: Alternative dispute resolution schemes**

67 The Australian Government, in recognising the important role played by Alternative Dispute Resolution (ADR) schemes, and in an attempt to formalise advice already given by the Office, should consider:

- amending NPP 2 to enable use and disclosure of personal information to ADR schemes in the course of handling disputes
- amending NPP 10 to enable collection of sensitive information where it is necessary for the investigation and resolution of claims under an ADR scheme
- defining the term ‘Alternative Dispute Resolution Scheme’ for these purposes in the Act.

7.13 **Responding to large scale emergencies**

**Introduction**

The Terms of Reference to the Review ask to what degree the private sector provisions meet their objects whilst recognising that privacy must be balanced against a range of other community and business interests including the general desirability of a free flow of information. The degree to which the NPPs meet this delicate balance was tested during the aftermath of the tsunami disaster in December 2004. In an attempt to locate missing family and friends, many Australians contacted airlines to find out whether the missing had continued flying after the tsunami hit. Such information, which is readily available to the airlines, if disclosed would normally appear to be a breach of NPP 2. The aftermath of the tsunami placed organisations in the position of balancing the right of an individual to privacy while also having the capacity to allay the fears of many relatives and friends of those missing.

Disclosure of personal information by airlines in situations such as presented by the tsunami could therefore be in breach of NPP 2.

**Law and policy**

**Privacy Act**

NPP 2.1 provides limited circumstances where an organisation may disclose personal information. NPP 2.1 allows an organisation to disclose personal information in situations such as where the individual has consented (NPP 2.1 (b)), where the disclosure is a related secondary purpose and within the
individual’s reasonable expectations (NPP 2.1(a)) and where the disclosure is authorised or required by or under law (NPP 2.1(g)). NPP 2.4 allows for personal information to be disclosed to a person who is responsible for compassionate reasons, however, this relates only to health information held by a health service provider.

**Issues**

The scale and gravity of large scale emergencies have tested the application of the Privacy Act and raised questions as to how privacy protection should operate in such situations. The Privacy Act received criticism in the media after the tsunami disaster for lacking commonsense and for being unable to anticipate and cope with the extent of the tsunami disaster\(^{206}\).

**What submissions say - addressing the issues**

One submission (confidential) argued in favour of amending the NPPs to enable organisations to disclose personal information to agencies or law enforcement bodies involved in coordinating the response in the event of an emergency or natural disaster.

**Options for reform**

**Temporary public interest determination**

Under section 80A, the Privacy Commissioner may make a Temporary Public Interest Determination (TPID) if the Commissioner is satisfied that the act or practice of an organisation breaches or may breach an NPP and the public interest in the organisation doing the act, or engaging in the practice, outweighs to a substantial degree the public interest in adhering to that Principle.

A possible solution to the kind of situation created by the tsunami is for the Privacy Act to be amended to enable the Privacy Commissioner to issue an emergency TPID. Once such a TPID is issued, disclosures that would ordinarily breach the NPPs would not be in breach during the operation of the TPID.

Currently, in order for a TPID to be created, an application needs to be made by an agency or organisation (section 73). Rather than requiring an organisation or agency to apply for a TPID, it may be more practicable and in the public interest for the Privacy Commissioner to issue a special emergency TPID without an application in situations where the public interest clearly outweighs any invasion of privacy.

\(^{206}\) See Daily Telegraph Friday 14 January 2005 p33.
Amend NPP 2 - Disclosures on compassionate grounds

Another option may be to include an exception to NPP 2 which would allow for disclosure based on compassionate reasons in times of national emergency. As noted above, NPP 2.4 enables a health service provider to disclose personal information to a ‘person responsible’ where the individual is unable to consent to the disclosure and the disclosure is made for compassionate reasons and is not contrary to any wish expressed by the individual.

Under NPP 2.4 a ‘responsible person’ includes a parent, child, sibling, spouse, guardian, power of attorney or person nominated by the individual to be contacted in case of emergency. NPP 2.4 could form the basis of an exception to disclosure in times of national emergency.

Parliament may wish to consider whether there is a social interest in having this information available to a ‘person responsible’. The extent of such disclosure needs further analysis. Consideration needs to be given to whether there is a public interest in restricting such disclosure to immediate family or if information should be disclosed more broadly, for instance to extended family and friends of a missing person. Whether there is a public interest in the media having access to such information is another option to be considered.

Taking into consideration the trauma suffered by families and persons responsible during times of national emergencies, it would be desirable to extend the definition of ‘person responsible’ to include those that families nominate to represent the family in times of trauma.

Amend NPP 2 - Disclosures in the Public Interest

Section 8(2) of the Canadian Privacy Act (R.S. 1985, c.P-21) states:

Subject to any other Act of Parliament, personal information under the control of a government institution may be disclosed (m) for any purpose where, in the opinion of the head of the institution,

(i) the public interest in disclosure clearly outweighs any invasion of privacy that could result from the disclosure, or

(ii) disclosure would clearly benefit the individual to whom the information relates.

If the Privacy Act were to have a similar section, it could clearly be invoked during a large scale emergency such as the tsunami. This section does not limit to whom the disclosure can be made. In adopting such as section, consideration would need to be given to whether such an exception is appropriate for information held by private sector organisations.
Involvement of government

Concerns about private organisations having to determine whether the public interest in disclosure outweighs the invasion of privacy could be addressed by involving government agencies such as the Department of Foreign Affairs and Trade (DFAT). DFAT has a high public profile in emergency situations and the community has an expectation that it will co-ordinate efforts to locate and assist in times of national emergencies. One option is to give a government agency such as DFAT the authority to collect this information and subsequently distribute the information to families and other appropriate persons or organisations.

Define ‘national emergency’

After the Bali bombings on 12 October 2002, an emergency amendment to Division 11A, Part 1D of the Crimes Act 1914 was made in order to assist in the identification of victims of the bombings. The Division was also amended to enable the Minister to make a declaration in the case of a national emergency or where Australians have died as a result of an incident occurring overseas. The Minister made a determination for the tsunami on 30 December 2004.

The Privacy Act could refer to ‘incidents’ as determined by the Minister under section 23YUF of the Crimes Act. Alternatively, the Privacy Act could be amended to include such a definition.

7.14 Recommendations: Large scale emergencies

Privacy laws should take a common sense approach. There needs to be an appropriate balance between the desirability of having a flow of information and protecting individual’s right to privacy. In developing an exception to disclosure for cases of national emergencies, consideration should be given to the seriousness of the privacy breach versus that of protecting privacy.

In large scale emergencies, the consequences of disclosure should be compared to the consequences of non-disclosure. Consideration also needs to be given to the potential identity fraud that may occur during such a time, especially if disclosure is allowed to the media.

The Australian Government should consider:

---

207 Section 23YUF(2A)(c) of the Crimes Act 1914.
• amending NPP 2 to enable disclosure of personal information in times of national emergency to a ‘person responsible’
• extending the NPP 2.5 definition of ‘person responsible’ to include a person nominated by the family to act on behalf of the family
• amending the Privacy Act to enable the Privacy Commissioner to make a Temporary Public Interest Determination without requiring an application from an organisation
• defining ‘National Emergency’ as ‘incidents’ determined by the Minister under section 23YUF of the *Crimes Act 1914*. 
8 New technologies

8.1 Developments

The NPPs were intended to be technology neutral to ensure that they would remain relevant despite technological change. The explanatory memorandum for the private sector provisions says:

‘The speed at which electronic commerce is evolving and changing makes it difficult for existing laws to be adapted. Any arrangements that are put in place need to provide an adequate and enforceable level of security and protection of personal information, while being flexible and technology-neutral so they can adjust to changing circumstances and emerging technologies’. 209

Since they were developed there have been some dramatic changes in technology that have had a considerable impact on the ways that personal information can be collected, tracked, connected and disclosed.

Telecommunications and internet

In the telecommunications area, new mobile phone technology and Radio Frequency Identification (RFID)210 technologies have emerged that can become means of tracking the movements of individuals or subjecting them to covert surveillance. Other new technologies such as Electronic Number Mapping (ENUM)211 and Voice over Internet Protocol (VoIP)212 are also leading to much greater connectivity and global reach. This enables many more organisations to have access to information about telephone numbers, including mobile phone numbers and related information. This may be unprotected by telecommunications legislation that has regulated telephone numbers in a more conventional environment. Mobile phone cameras have also become widely available. Much of this technology is available to, and used by, individuals as well as organisations.

An increasingly wide range of transactions are carried out online. The nature of such technology means that every transaction leaves a data trail that can potentially be followed by someone else.

209 Privacy Amendment (Private Sector) Bill 2000 Revised Explanatory Memorandum – Senate, November 2000 p 9
210 Radio Frequency Identification or Radio Frequency Identification tag(s) uses wireless technology to transmit product serial numbers from tags to a scanner, without human intervention. It is regarded as a likely successor to barcode inventory tracking systems.
211 ENUM is a communications protocol that links the public switched telephone network (PSTN) with the Internet by translating telephone numbers into a format that can be used by the Internet.
212 Voice over Internet Protocol, is another way of saying IP Telephony. It involves the transmission of telephone calls over a data network like the Internet. In other words, VoIP can send voice, fax and other information over the Internet, rather than through the PSTN or regular telephone network.
A research paper prepared for the Council of Europe in late 2004 on the application of data protection principles to the world wide telecommunications networks outlines a range of developments that mean that:

‘. . it has and will become more and more possible to record the details of all the individuals on our planet and this will be less and less visible.’213

Data aggregation and mining

Technology has also made it much easier to connect information, such as a telephone number, with an individual’s name or other contact information such as a postal or email address. Also, people can be more easily contacted, for example, by email, without the need for a name.

Media around America’s largest data miner ChoicePoint shows the breadth of personal information that new technologies have allowed organisations to collect and the indirect means by which they collect it. It also shows the vulnerability of these huge data warehouses and the privacy threats they pose.214 ChoicePoint’s computers hold 19 billion data files that include names, addresses, social security numbers, phone numbers, driver’s licences, car registrations, credit histories, birth certificates, real estate deeds, legal histories, fishing licences, military records, insurance claims, thumbprints, and DNA. It accumulated this information as a result of buying a series of well targeted businesses. It attracted media attention when it became public that it sold information about 145,000 people to a person posing as several small-business owners who used the information to create fraudulent identities. Clients of ChoicePoint range from the boy scouts to the CIA.215

Biometrics

Another development is the increasing use of biometrics for identity management. Biometric technologies are being used in a range of contexts in both the public and the private sectors. For example, biometric technologies in the private sector are being used or proposed for identification purposes in methadone programs, taxi booking services, ATMs and online banking, access to buildings and many others.

214 See for example, article in Time Australia, 7 March 2005 ‘Are your secrets safe?’ Also, "Not the first time for ChoicePoint", MSNBC, 27 Feb 2005.
215 Time Australia, 7 March 2005 ‘Are your secrets safe?’
Drivers for the use of biometric technology include the increasing power of information technology, increasing remote communications requiring identification and authentication, commercial and national security issues and increasing interoperability between biometric systems and between biometrics and other systems.

The collection and use of biometric information has great potential to contribute to the protection of personal information and identity, but it also has the potential to pose great privacy risks. Biometrics can be a powerful identifier. Whether it poses privacy risks depends on whether:

- biometrics are used to accumulate or link large amounts of personal information in a central place
- people have choice about whether to provide biometric information
- biometrics are used to collect information covertly
- there are procedures for when things go wrong and
- there are built in protections against function creep.

Privacy risks are most likely to arise where individuals have no choice about the use of the technology and the process lacks openness and accountability.

**Electronic health records**

Significant developments in the areas of e-health and electronic health records have notable implications for privacy, including for the private health sector.

A number of electronic health records systems are being developed at the local, regional and national levels. Some states are developing these systems, such as OACIS in South Australia and Health e-link in New South Wales (formerly EHR*Net). At the national level, the HealthConnect project aims to create a centralised system for managing information (in summary form) about individuals' interactions with the health sector.

The Australian Government has also provided funding to help health service providers (particularly general practices) obtain high-speed broadband internet connections. This will help facilitate their participation in initiatives such as HealthConnect.

**Role of technology in protecting privacy**

There is a role for technology itself in protecting privacy, often called Privacy Enhancing Technology or PETS. For example, a system can be built to allow anonymity, or it can be built in a way that identifies every step a user takes:

218 http://www.healthconnect.gov.au


“At the University of Chicago, it is possible for students, staff and administrators to communicate anonymously. If one wants access to the Internet, one can simply connect one’s computer to any Ethernet connection jack located throughout the University. At Harvard, however, a machine cannot be connected unless it is registered, so that all interactions with the network can be monitored and identified with a particular machine, and probably a user.” \(^{219}\)

Generally speaking, commentators see the use of PETs as a useful complement to legislation, regulation and the education of individuals to take protecting action for themselves.

As currently framed, the private sector provisions do not impact on those developing new technologies because they generally are not handling personal information in the process.

**Issues**

The issues paper raised the general question of whether the private sector provisions are adequate in protecting individual privacy in the light of these developments. It also raised particular issues including whether:

- it is possible to maintain the technological neutrality of the provisions
- the ability to identify individuals should remain as the focus for privacy protection
- the provisions should extend to the activities of individuals acting in their private capacity and
- confidence in privacy protection in new technologies is impeding commerce in this area.

**8.2 What submissions say – the issues**

**Support for technological neutrality**

There is significant support in submissions for the concept of maintaining the technological neutrality of the NPPs to ensure that they remain relevant despite technological change. \(^{220}\) However the Australian Communication Authority (94) says that given the rapid rate of change there is a need to periodically review the adequacy of the NPPs on this point. Baycorp (86) says that its experience is that the neutrality of the NPPs supports...

---


\(^{220}\) See for example, Fundraising Institute of Australia FIA 52, Coles Myer 60, Association of Market Research Organisations (AMRO) and the Australian Market and Social Research Society (AMSRS) 61, Australian Direct Marketing Association 67, SENSIS 84, Baycorp 86, ACA 94, Optus 98, Telstra 110, Australian Retailers Association 111, Vodafone 112.
technological change and while there is a need to examine the privacy impact of new technologies there should be no regulatory change unless it meets very stringent tests. Australian Business and Specialist Publishers (8) suggests that new technology does not necessarily mean privacy infringement and says that there should be no change until there is a proven problem.

Submissions are mixed however on whether the intrusiveness of a technology is a privacy issue. For example, the Australian Direct Marketing Association (67) recognises:

‘the OFPC’s concern that some contact channels and technologies are more intrusive than others – indeed, this is reflected in ADMA’s ‘hierarchy on intrusion’ which recognises that the more invasive the contact channel, the higher level of protection required. However, ADMA does not believe that this is a privacy issue – instead it is about use of technology. . . . the purpose of the private sector provisions is not to regulate how an organisation uses technologies or channels to contact individuals, it is to regulate how an organisation handles personal information.’

Baycorp (86) says, in its experience, that regardless of the channels used to contact individuals, businesses have remained focused on the individual’s right to privacy.

On the other hand, although it supports technological neutrality, Optus (98) considers that there are new and emerging technologies, such as VoIP and IP and Location Based Services that may provide new challenges for the protection of Australian consumer information because the functionality that these services provide is more invasive.

In the case of VoIP, Optus (98) says that for the first time ever the Australian public will be able to access voice services from a provider that has no presence or dealings in Australia. It raises the privacy issues associated with ENUM registries operating in the VoIP environment, which will contain details of telephone numbers and IP addresses as well as possibly details of service preferences and settings for additional calling features. It recognises the importance of having a suitable framework which the Australian Communications Authority has already begun to develop. It also warns that low cost services such as these should not mean less privacy protection and that VoIP providers will need to be aware of the privacy of both originators and receivers of these types of calls. It is also concerned that neither the Privacy Act nor the Telecommunications Act may cover VoIP providers that are overseas and that there is a need to consider whether the Office has the ability to ensure that overseas VoIP providers comply with the NPPs and to raise consumer awareness of these issues.

The Australian Consumers’ Association (15) considers that the Privacy Act is not working because it cannot deal with the technologically specific risks of certain new technologies. It cites the examples of the Spam Act, and industry
codes such as the ACIF Short Message Service (SMS) code and the ADMA m-commerce codes as examples of this.

**Gaps in the private sector provisions and new technology**

**Location based technology**

The emergence of location-based technology, for example location based services for mobile phones, RFID or the Global Positioning System (GPS) capabilities of some mobile phones, was raised by a number of submitters who suggest it may pose a challenge for privacy regulation\(^{221}\). The Australian Consumers’ Association (15) argues that the current Privacy Act does not clearly establish consumer control over location information and challenges assumptions about how privacy and personal information inter-relate. It says that unless the individual controls the context in which the information is released, a business making an unsolicited locational approach will have a high probability of being inappropriate, intrusive and quite possibly offensive.

**MCommerce**

MCommerce (mobile commerce) may raise new privacy challenges, including consideration of the security of transactions. For example, sensitive financial information such as credit card details may be sent using unencrypted SMS messages. The Australian Communications Authority (94) suggests that consideration be given to amending NPP 4.1 to state that service providers should ensure the payment mechanisms they establish also protect the personal information of consumers.

**Spyware**

Spyware is another emerging technology submissions raise as having significant privacy implications. The Australian Consumers’ Association (15) argues that consumers should have an enforceable right to know who is watching them, and to make them stop if they do not like it unless the watcher has some overriding authorisation such as a court order or warrant.

Another use of technology to ‘spy’ on others is the use of ‘scanners’ to listen to radio communications by emergency services. The Australian Communications Authority (94) notes that it has received complaints regarding the use of scanners to listen to police frequencies where the information obtained is then used inappropriately. In many cases this sort of incident would not covered by the Privacy Act because it is carried out by individuals in their personal capacity, and because it may not result in collection of information for inclusion in a record.

---

\(^{221}\) Australian Consumers’ Association 15, Australian Communications Authority 94, Optus 98.
The Department of Communications, Information Technology and the Arts (DCITA) released the results of a legislative review into the coverage of existing laws regulating spyware in March 2005\textsuperscript{222}. It found that the most serious and malicious uses of spyware are already covered by existing legislation. DCITA is planning to undertake public consultation on spyware in May of this year.

**Health issues**

A number of submissions are concerned that the NPPs may not adequately keep pace with the use of new technology in the management of health information in the health sector, such as through electronic health records systems.

The Australian Physiotherapy Association (37) says that with greater use of electronic methods of information transfer, there comes a need for greater levels of awareness about how to protect health and other personal information.

The Pharmacy Guild of Australia (93) is concerned that the NPPs may not be adequate for these new systems, including because they can create more avenues for the transfer of health information to more organisations. Similarly, the Australian Federation of AIDS Organisations Inc (54) submitted that ‘electronic sharing of health information raises the potential for sharing of information across a wide network and consumers may feel that they quickly lose control of who has access to their records’.

Also, the Australian Government Department of Health and Ageing (99) noted:

> ‘as personal information becomes more widely dispersed and stored on larger databases, it may potentially become more difficult for an individual to control the flow and exchange of personal information unless proper privacy safeguards are built in from the outset.’

The Department of Health and Ageing (99) also expresses concerns about privacy protection where an e-health website, used by a consumer, is located overseas.

**Other gaps arising from new technology**

Xamax Consultancy (3) says that the private sector provisions fail to address the greatly heightened privacy-invasiveness, and the new technological threats, that has been a feature of the 25 years since the promulgation of the OECD guidelines in 1980 on which the NPPs are based. These include that they do not:

\textsuperscript{222} Outcome of the Review of the Legislative Framework on Spyware

provide individuals with control over ‘their’ identification and authentication tokens (such as chip-cards and digital signature keys)
provide the necessary tight regulatory regime over the use of biometrics
address rampant surveillance technologies, or force corporations to achieve balance between their desires and those of individuals
impose a responsibility to ensure that an automated decision that is adverse to the interests of a consumer is subject to review by a human being before being communicated or implemented.

Activities of private individuals

Individuals now have greater access to a wide range of technologies that can have considerable potential to be privacy invasive.

However, there does not appear to be a great deal of support from submissions, or in consultations, for changing the Privacy Act so that it covers the activities of private individuals in their personal capacity. For example, the Australian Consumers’ Association (15) says that controlling individual behaviour is best left to social norms backed by general or specific laws.

On the other hand, the Australian Communications Authority (94) says it has received complaints regarding the use of scanners by individuals in their private capacity to listen to police frequencies where the information obtained is then used inappropriately. It supports further consideration being given to how to address the issue of protecting invasions of individual privacy by individuals acting in their private capacity.

Definition of personal information

The changing nature of technology also raises the issues of whether the definition of personal information adequately covers the activities that might be considered to be privacy invasive in this new environment.

Concern about changing definition

A number of submissions are not in favour of changing the definition of personal information\textsuperscript{223}. The costs associated with change are an issue\textsuperscript{224}. Vodafone (112) says that maintaining consistency with privacy regimes in the United Kingdom and Ireland is another reason for no change to the definition. Coles Myer (60) says:

\textsuperscript{223} See for example, Virgin 26. Coles Myer 60, Optus 98, Telstra 110, Vodafone 112.
\textsuperscript{224} See for example, Telstra 110.
‘We accept the proposition of some privacy and consumer advocates that this principles-based approach can lead to uncertainty from a consumer perspective. It is true that two similar fact scenarios may lead to different privacy outcomes depending on whether or not an individual can be identified. Coles Myer does not believe this is a short-coming of the Act. Instead, it requires each situation to be assessed on its individual merits rather than a blanket rule to be applied. This is the appropriate analysis given the Act’s concerns to protect individual rights, rather than public rights in general.’

An example of when similar fact scenarios may lead to different outcomes is raised by the Department of Health and Ageing (99). The Department says that the move toward personalising the provision of health information online raises questions about whether the advice provided by an ehealth site amounts to ‘treatment’ rather than preventative information or promotion. If the site is providing treatment, then they become a health service provider. It asks the question in relation to consumers using such services:

‘... if they are receiving ‘online treatment’ through a fully automated CBT [Computer Based Treatment] intervention are they entitled to the same legal rights and protection as a consumer receiving CBT in the GP surgery, including privacy rights?’

It suggests that the answer to this question may depend on whether the email address used by the individual accessing such sites can be characterised as personal information.

In relation to the issue of whether the ‘ability to contact’ an individual should form part of the focus of privacy protection, Baycorp (86) says it is mindful that when first enunciated, the right to privacy was expressed as a ‘right to be let alone’. Further it says:

‘But as the information economy has been developed, it has become very clear that the principal means that value is created in that economy is by the association of previously disparate elements of information. Much of that data relates to individuals. Accordingly, Australia, like other jurisdictions, has restricted its privacy regulation in two important ways:

- it does not confer an absolute or presumed right to anonymity
- it is limited to the individual’s rights over the collection and use of personal information.

These restrictions in scope are fundamental to an enabling technologically neutral environment. Without them, the privacy regime could easily inhibit the development of an information economy in Australia.’
Baycorp goes on to say that any proposal to extend the scope of privacy regulation to include the ‘right to be let alone’, should only be carried out if it meets stringent tests which establish both serious harm and the absence of any alternative, non-regulatory response. It says the current examples do not meet this test.

Concerns about current definition of personal information

On the other hand, other submissions\textsuperscript{225} identify a number of issues relating to the current definition of personal information which might support a need to move privacy protection away from the current concept of identification, as represented in the privacy framework.

The Australian Communications Authority (94) recognises that although the Privacy Commissioner generally does not consider that mobile telephone numbers and ‘generic’ email addresses which do not clearly identify an individual are ‘personal information’, it has been the Australian Communication Authority’s experience in enforcing the Spam Act that individuals affected by spam regard their telephone numbers and email addresses as personal information and the receipt of spam as a violation of individual privacy.

The Australian Communications Authority (94) goes on to say that:

‘While individuals may move away from traditional identifiers, the new protocols such as email addresses, avatars and internet banking passwords may be no less indicative of identity. As lives are increasingly led ‘online’, identifiers may not bear a resemblance to traditional physical concepts of identity.’

The Communications Law Centre (72) says that the narrow definition of personal information is a key problem, as it allows organisations in the online world to create user profiles that monitor and keep track of individuals’ habits and interests but that are not regulated by the NPPs. Electronic Frontiers Australia (51) supports this view:

‘On the internet, it is not necessary for businesses or any other online service to be able to reasonably ascertain the actual identity of an individual, in order to build a profile about them. All that is necessary is a sufficiently unique identifier. Such identifiers (and profiles) may be disclosed to other entities who are able to connect a ‘cyberspace’ identifier with a name or other “real-world” identifier.’

Confidence in privacy protection

Few submissions comment on the question of the level of community confidence in the online environment, or the reasons behind this. Telstra

\textsuperscript{225} For example, the Australian Communications Authority 94, Electronic Frontiers Australia 51, Communications Law Centre 72.
(110) says that if confidence is undermined, raising awareness is the answer. However, several other submissions suggest that the low level of trust of individuals in internet companies is probably justified and that encouraging the community to think otherwise would be misleading. Electronic Frontiers Australia (51) says:

‘The fact is that, under existing Australian law, individuals have almost no privacy “rights” in the online environment and even the few rights they allegedly have are not protected adequately and are difficult, sometimes impossible, to have enforced. The lack of rights arises from a combination of factors, including but not limited to, uncertainty regarding the definition of “personal information”; no requirement to obtain consent before collecting personal information; use of bundled “consents” including to disclose information to unspecified “partners”; the small business exemption; and/or technological developments.’

The Australian Consumers’ Association (15) and Electronic Frontiers Australia (51) suggest that an important way to encourage community confidence would be for the Office to take more vigorous and apparent enforcement action.

8.3 What submissions say – addressing the issues

Addressing new technology generally

Special legislation

During consultations it was recognised by many that the NPPs will not always be able to deal with every privacy invasive situation. However, in general, there was a view that in this case, it was better to deal with it in special legislation, rather than amend the NPPs. For example, Telstra (110) says:

‘If existing privacy laws are found to be lacking with respect to the application of a particular technology, then it is better to deal with the relevant issue in specific legislation rather than by amending the general principles in the NPPs. Telstra notes that this was the approach adopted to address the issue of unsolicited electronic communications by the Commonwealth Government (i.e. through introduction of the Spam Act). The NPPs are intended to provide a set of general guiding principles rather than exhaustive legislation on privacy issues.’

Office involvement in oversight of technologically specific legislation

Nonetheless there is also concern that if channel/technology specific legislation is developed by government, that the Office should play a more
active role in ensuring that such legislation reflects both the definition requirements of the NPPs and does not introduce conflicting obligations on business. Others are less sure that specific legislation is necessarily always appropriate.

Enforceable national guidelines

Coles Myer (60) suggests that one way to deal with any failings in the national approach to technology would be to have enforceable national guidelines or an industry code applying horizontally to certain issues. In this vein, the Australian Retailers Association (111) is developing an RFID consumer code which specifically mentions and operates in accordance with the NPPs because the NPPs cover the applications of the technology regardless and cannot be negated. It agrees with ADMA that it is the information that matters, not the technology.

Office to engage broadly with the community

Vodafone (112) believes that the best approach to addressing issues relating to new telecommunications technologies is for the Office to support the regulatory principles of technology neutrality and to engage broadly with the telecommunications industry and relevant authorities.

Addressing issues about health records

Specific regulation for electronic health records

In response to the challenges they raise for the NPPs, a number of submissions suggest there should be specific privacy protection for electronic health records.

The Australian Nursing Federation (127) submits that national standards should be developed specifically for electronic health records, and that these should complement privacy. It argues that technologically neutral privacy principles or legislation could leave consumers at risk.

The Australian Federation of AIDS Organisations (54) proposes that specific provisions be inserted into the Privacy Act to guarantee that consumers have a choice of voluntary participation in such systems. Also, these provisions should require health service providers to inform consumers of their rights when participating in such systems.

The Australian Medical Association (29) says there should be stronger provisions in the law and greater resources at the federal level to prevent corporate misconduct around the on-selling of health information. For

---

226 See for example, ADMA 67, Fundraising Institute of Australia 52.
227 See for example Australian Consumers’ Association 15 in relation to RFID.
228 For example, AMA 29, Pharmacy Guild of Australia 93 and AFAO 54.
example, it questions whether ‘so-called’ de-identified data is genuinely de-identified, or how easily it can be re-identified.

A number of submissions stated that the Privacy Commissioner should be represented on key, national e-health forums, including HealthConnect and the National e-Health Transition Authority.\(^{229}\)

**Consistent regulation for electronic health records**

Submissions state that the multiple sources of privacy regulation in Australia pose challenges for a national electronic health records system. For example, the Department of Health and Ageing (99) describes the current regulatory environment as a ‘patchwork’, which ‘creates major problems for the future of national e-health initiatives’.

However, one submission says that prescribing privacy protections into law for HealthConnect may prove problematic when information is shared with other health records systems. Prescribed protections for the respective systems need to be consistent for their interoperability to be successful.\(^{230}\)

The consistent implementation of a National Health Privacy Code (see Chapter 2) across all jurisdictions could provide baseline conformance in privacy protection in this area. However, any specific legislation governing the operation of electronic health records systems also needs to be consistent across all systems.

**Change to definition of personal information**

To address the issue of use of identifiers to profile individuals and then connect the profile to a name, Electronic Frontiers Australia (51) says that the definition of personal information must be extended to cover identifiers irrespective of whether it is obvious to the collector or discloser that an individual’s identity can reasonably be ascertained from that identifier and whether or not an individual can be contacted by use of that identifier. It recommends that the definition of personal information in the Privacy Act be extended to include wording such as:

‘Any information which enables interactions with an individual on a personalised basis, or enables tracking or monitoring or an individual’s activities and/or communication patterns, or enables an individual to be contacted’.

The Australian Privacy Foundation (90) supports an ‘ability to contact’ test perhaps by adding wording along the lines of ‘“... or information sufficient to allow communications with a person”, that is, whether or not it is sufficient to allow the person to be identified.’

\(^{229}\) Relevant submissions include AMA 29, and Australian Nursing Federation 127.

\(^{230}\) South Australian Department of Health, ICT Services 53.
On the other hand, a number of submissions favour making no change at all, or only if there is clear evidence of a need which cannot be addressed in other ways.\textsuperscript{231}

\section*{Senate inquiry}

On 9 December 2004 the Senate referred a number of matters relating to the Privacy Act to the Senate Legal and Constitutional References Committee. The terms of reference include that the Committee is to look at ‘the capacity of the current legislative regime to respond to new and emerging technologies which have implications for privacy’. The terms specifically refer to smart card technology, biometric imaging data, genetic testing and microchips that can be implanted in human beings.

There may be information relating to new technology presented in the Senate inquiry that may be relevant to this, and any subsequent wider inquiry into the Privacy Act.

\section*{8.4 Options for reform}

\subsection*{Maintain technological neutrality of the NPPs}

NPPs may not be technologically neutral

Submissions generally support maintaining technological neutrality for the NPPs. There are strong arguments for doing this. Unless neutrality is maintained, the NPPs would need constant change to accommodate every new technology. Legislative change could not keep up with this. It would also make the NPPs more prescriptive.

However, submissions received and also work that is taking place globally indicate that the NPPs as they currently stand may not in fact be technologically neutral. They are based, with some modifications, on the OECD principles that were developed during the 1970s when the electronic and telecommunications environment was vastly different from what it is now. In particular, the NPPs do not appear to have been developed with the online environment in mind. For example, there do not appear to be provisions which take into account the identifiers used in the online environment (resulting from packet switching rather than circuit switching) and the uses that can be made of them to track the transactions of an individual. The provisions do not take into account the different approach to identity authentication required in the online environment.

Also, the NPPs rely on people making informed choices about whether, and how much, information about themselves they hand over. In the online environment, people may have very little knowledge or choice about some of

\textsuperscript{231} For example, Virgin 26, Coles Myer 60, Optus 98, Telstra 110, Vodafone 112.
the data trails they leave. On the other hand, gaining an individual’s consent to some specific activities in relation to personal information is much easier than in the paper based environment.

As online and electronic interaction becomes increasingly a key part of people’s lives, it becomes more difficult to argue that privacy principles that do not take into account these realities are technologically neutral.

**EU research**

Support for this view can be found in research carried out for the Council of Europe which states:

‘The advent of the Internet has created a need for a third generation of data protection regulations’.\(^{232}\)

This suggests that there may be a need for new NPPs to accommodate these realities. For example, there may be a need for organisations to give people choice about the kind of identity authentication that they are to use, or there may be a need for organisations to only engage in profiling activity if they have the consent of the individual.

**Issue is complex**

These are complex issues that have not been researched or canvassed fully in the course of this review. Any change in the NPPs should only be done after appropriate consultation with stakeholders. This may best be done in the context of a wider review of the Privacy Act.

**Change definition of personal information**

Adding new NPPs to the private sector provisions may address some of the emerging privacy challenges of new technology. However, it appears that the current definition of ‘personal information’ may be an impediment to the ability of the private sector provisions to address these challenges.

Whether or not a person’s identity can be reasonably ascertained from information is becoming difficult to determine. With the advent of new technologies it is increasingly difficult to conclude that information that may appear to be de-identified, or not identified can never be connected with a real person. There is evidence that information about people is increasingly used to make contact with people in ways that people find privacy invasive even if it cannot necessarily lead to the physical location of individual or their actual name (for example, email). It is also being used to profile individuals.

As the Council of Europe research suggests:

‘New technology makes it increasingly possible to process data relating to individuals not, as was traditionally the case, through data relating to their legal identity, such as name and address, but via an anchor point or even an object (so-called ambient intelligence) associated with it. This means that the danger often no longer resides in the collection of personal data as such but in the subsequent application of abstract profiles to individuals.’

The European research report says that it is clear that the Consultative Committee will have to work with the concept of personal data. It concludes:

‘A definition of personal data based on undefined and indefinable notion of identity and the pendant concept of anonymity is ambiguous and not directly workable. From the practical point of view, it would be better to refer to biographical data, identifiers linked to individuals or to terminal (indeed objects), and points of contact.’

Changing the definition of personal information would be a major step and could have major implications for business. Once again, it is a complex matter and requires research and consultation. For example, the UK Information Commissioner recently commissioned research on the issue of ‘What are personal data?’ This could be a matter appropriate for a wider review of the Privacy Act.

**Issue guidance on definition of personal information**

The Office could issue further guidance consistent with existing law on what is personal information which takes into account the fact that in the current environment, it is more difficult to assume that any information about people cannot be connected. It is not clear that this would solve the ‘ability to contact’ issue.

**Specific legislation for electronic health records**

The benefits are attractive, but the privacy risks posed by electronic health records systems could be high due to the capacity of such systems to link

---

235 ‘What are Personal Data: A study conducted for the UK information Commissioner by Sharon Booth, Richard Jenkins, David Moxon, Natasha Semmens, Christopher Spencer, Mark Taylor.'
highly sensitive information and to make it more widely accessible. If things go wrong with such a system, the implications could be severe.

The security and governance arrangements for these systems need to be assured. Also, individuals who choose to take part in these systems need to retain adequate control over how their information is handled.

Therefore, as well as having a national standard for protecting the handling of health information (that is, a consistently enacted National Health Privacy Code), there appears to be a need for specific enabling legislation for electronic health records systems generally. This is the case particularly for an overarching national (or enabling) system, such as HealthConnect.236

**Process to address global issues**

The advent of new technology has added urgency to the need to take a global approach to privacy protection. The Government should initiate discussions about how to deal with major jurisdictional issues arising from the global reach of new technologies such as VoIP. There needs to be a globally consistent approach to new technologies in these areas and a chance for individuals to have recourse if their information is inappropriately used. The consequence of not having a globally consistent approach is that information may end up in the country with the lowest privacy protection standards.

**Power to initiate binding codes**

The Office could make use (when necessary) of any new powers to initiate binding codes (see recommendation 7) to deal with technologically specific situations.

This would enable the Government and the Office, where appropriate, to respond quickly to emerging privacy issues in the area of new technologies. However, there are considerations to be addressed including, unless the NPPs are updated, could a code deal with areas not necessarily covered by the NPPs, for example, use of identifiers or profiling.

**Promote privacy impact assessments and privacy enhancing technologies**

Protecting privacy in the face of rapidly developing new technologies requires a range of strategies.

There could be a greater role for the Privacy Commissioner to raise awareness among those developing new technologies about the need to build

---

in privacy and the considerations that need to be taken into account so that technology is developed in a way that is privacy enhancing rather than privacy invasive.

One way that is increasingly being used to assess and avoid the privacy risks inherent in many large scale projects involving new technologies is to conduct privacy impact assessments. The Office is developing privacy impact assessment guidelines for public sector agencies. This approach could also be applicable in the private sector.

The Office could encourage technology developers and implementers to conduct a privacy impact assessment for large scale high privacy risk projects. A wider review of the Privacy Act could consider the question of whether the Privacy Act should include provisions which provide for a privacy impact assessment to be carried out in specified circumstances.

**Review definition of personal information and need to update model to take into account new technology**

Some of these issues are complex and need more detailed consideration. One approach is to deal with most of the above by including it as part of a wider review of the Privacy Act.

---

237 A Privacy Impact Assessment (PIA) is an assessment tool that describes, in detail, the personal information flows in a project, and assesses the privacy risks a project may pose. The purpose of a PIA is to gain an understanding of, and to minimise, any adverse impacts a project may have on the privacy of individuals. A PIA may do this for example, by helping to identify when collection of particular information is unnecessary to a project, or where accountability or oversight processes may reduce privacy risks. It enables and organisation to:

- describe fully and systematically, the way personal information ‘flows’ in the project
- analyse how these information flows will impact on privacy
- consider alternative, less privacy-intrusive practices
- assess and manage privacy risks during project development rather than retrospectively
- identify early, a project’s potential for further privacy erosion, for example, through ‘function creep’ (additional uses of a system, and/or the personal information it involves, beyond the original plans or expectations) and
- make informed choices and recommendations about how the project will proceed.
### 8.5 Recommendations: New technologies

| 69 | The Australian Government should consider, in the context of a wider review of the Privacy Act (see recommendation 1) reviewing the National Privacy Principles and the definition of personal information to assess whether they remain relevant in the light of technological developments since the OECD principles were developed. This should ensure that the private sector provisions remain technologically neutral and relevant to protect data privacy in the main contexts in which information about people is currently collected, used and disclosed. |
| 70 | The Australian Government should consider initiating discussions through appropriate international forums about how to deal with major international jurisdictional issues arising from global reach of new technologies such as Voice over Internet Protocol (VoIP). |
| 71 | The Australian Government should consider developing specific enabling legislation to underpin any national electronic health records system. The legislation should be consistent with the National Health Privacy Code, but also include enhancing protections for matters such as the voluntariness of the system and limitations upon the uses of people’s health records. |
| 72 | The Office will issue further guidance, consistent with the current law, on what is personal information which takes into account the fact that in the current environment it is more difficult to assume that any information about people cannot be connected. |
| 73 | The Office could use, if necessary, any new powers to develop binding codes (see recommendation 7) to deal with technologically specific situations. |
9 Clarifying how the National Privacy Principles work

9.1 NPP 1.3(d)

Law and Policy

NPP 1.3 sets out an organisation’s obligations to provide notice to an individual when collecting personal information from them.

The principle requires an organisation to take reasonable steps to give notice to the individual about a number of things, including the identity of the organisation, the fact that the individual can gain access to their information and why the organisation is collecting their information.

More specifically, NPP 1.3(d) requires an organisation to advise the individual about likely disclosures of their personal information to other organisations.

The issue

In the course of providing advice and guidance on the operation of the Privacy Act, the Office has found what appears to be an unintended gap in NPP 1.3(d). While this issue has not been raised in the review process, and appears to have been generally non-contentious, this can create uncertainty about how the principle operates.

The principle states that a collecting organisation must give notice to the individual about certain likely disclosures: these must be ‘usual’ disclosures and they must be to ‘organisations’. The complexity arises in the use of the term ‘organisation’ within the principle.

A general reading would suggest that the individual should be told about any entities or individuals to whom their personal information is likely to be given by the organisation collecting their information. This is consistent with the general intent of openness and transparency promoted by NPP 1.3.

However, the term ‘organisation’ has a specific and more limited meaning within the Privacy Act. Under section 6C, this term excludes such entities as small business operators, political parties and state or territory authorities. Instead, it defines which entities (or ‘organisations’) are covered by the private sector provisions.

If interpreted strictly, the principle could mean that an organisation collecting personal information would need to tell an individual about likely disclosures of their information only in respect of private sector businesses to which the private sector privacy provisions apply. They would not have to tell the person about likely disclosures to Australian Government, state and local
government agencies, private individuals or other entities such as small business operators.

This distinction seems to be inconsistent with the policy intent of the legislation. The Explanatory Memorandum in relation to this principle indicates that this distinction was not intended, when it says:

‘In relation to the requirement in 1.3(d) to tell the individual about the types of organisations to which the organisation usually discloses information of the kind collected from the individual: ‘Reasonable steps’, in this context, means giving generic descriptions of sets of organisations (for example, ‘debt collectors’ or State Government licensing authorities’ or ‘health insurers’)238.

The mention of state government licensing authorities, which do not fall within the definition of ‘organisation’ in the Privacy Act, indicates that a collecting organisation should tell the individual about disclosures to a far broader range of entities than ‘other organisations’.

**Options for Reform**

**Amend NPP 1.3(d)**

To provide greater certainty to business and individuals, and to ensure delivery of the policy intent of the principle, NPP 1.3(d) could be amended.

The principle could be revised to make clear that a collecting organisation must take reasonable steps to notify an individual of likely disclosures generally, whether these disclosures are to other ‘organisations’, to public sector agencies of the Australian Government or state or local governments, to other bodies or to private individuals.

**No change**

This issue did not figure in submissions and has been identified through the Office’s practice and experience in regulating with the NPPs. One option is to further monitor any issues that may arise with a view to addressing them later, if needed. However, this approach would mean that a known and unexpected uncertainty in the law, for which the policy intent appears clear, would not be resolved in a timely fashion.

---

9.2 Recommendation: NPP 1.3(d)

The Australian Government should consider amending NPP 1.3(d) to make clear that an organisation collecting personal information from an individual must take reasonable steps to notify them of likely disclosures generally, including to public sector agencies of the Australian Government, state or local governments, other bodies and private individuals.

9.3 NPP 1.3 and 1.5 - ‘reasonable steps’

Law and Policy

Under NPP 1.3 and NPP 1.5 an organisation collecting personal information from an individual, or from another source about the individual, must take ‘reasonable steps’ to ensure they are made aware of certain matters.

The issue

In the course of providing advice and guidance to business on the operation of the Privacy Act, the Office has identified some uncertainty about how these principles operate.

It is unclear whether an organisation can determine that, in some circumstances, taking no steps to provide notice to an individual is in itself reasonable. A number of organisations have raised circumstances with the Office in which it seems reasonable for them not to provide notice.

Therefore, the Office issued an information sheet\(^{239}\) to clarify where it may be reasonable to take no steps to provide notice. For example, this may be where significant cost or difficulty is involved in contacting a third party whose information has been collected incidentally, where a health service provider collects information about family members of an individual for inclusion in the person’s medical, social or family history, or in many circumstances where the information is collected from a public source.

However, the Law Council of Australia (36), while commending the guidance given by the Office about NPP 1.5, raises concerns that, without an amendment, a court may interpret the principle more narrowly. The Law Council of Australia suggests that the principles should make clear that in some circumstances taking no steps to provide notice would be reasonable in complying with the requirements in NPP 1.3 and NPP 1.5.

---

\(^{239}\) Information Sheet 18 - ‘Taking Reasonable Steps to Make Individuals Aware That Personal Information About Them is Being Collected’.
**Options for Reform**

**Amend NPP 1.3 and NPP 1.5**

To provide greater certainty to business and individuals, NPP 1.3 and NPP 1.5 could be amended to make clear that there are situations where taking no steps to provide notice to an individual will be reasonable.

This approach would ensure consistency between the legislation and the guidance provided by the Privacy Commissioner. This would not involve any change in business practice, and would create greater certainty. This approach may also assist in reducing the length of privacy notices.

**No change**

While this was not a high-profile issue in submissions, it was identified and has been a matter of significant discussion between the Office and a range of businesses over past years. Therefore, while one option would be to monitor the issue further, this would mean that a known uncertainty in the law is not resolved in a timely fashion.

**9.4 Recommendation: Reasonable steps for NPP 1.3 and 1.5**

The Australian Government should consider amending NPP 1.3 and NPP 1.5 to make clear that there are situations in which the reasonable steps an organisation might take to provide notice to an individual may equate to no steps.

**9.5 NPP 1.5 - collection from ‘someone’ else**

**Law and Policy**

NPP 1.5 requires an organisation to take reasonable steps to notify an individual if it collects personal information about them from someone else.

**The issue**

In the course of providing advice and guidance on the operation of the Privacy Act, the Office has identified some uncertainty about how this principle operates.
NPP 1.5 applies to the indirect collection of personal information from others, such as other individuals or businesses. However, there is uncertainty about whether it applies to collection from another source such as a newspaper or a book, a court report, or a CD produced by a company.

There are good policy reasons why the notice obligations in NPP 1.5 should apply to an organisation in some circumstances when it collects personal information from these kinds of sources. For instance, the source may contain sensitive information about the individual, which could be connected with other information or decisions relating to the individual. If they are not advised about the collection, this could occur and have a significant impact on the person’s life without his or her knowledge.

The Office developed, consulted widely upon and issued an information sheet, which interprets NPP 1.5 as applying an organisation’s notice obligations (where to do so is reasonable) to these sources, as well as to collection from other individuals, or organisations and agencies. The information sheet has gained widespread acceptance.

**Options for Reform**

**Amend NPP 1.5**

To give greater certainty to business and individuals, NPP 1.5 could be amended to make clear that an organisation has notice obligations when collecting personal information indirectly (that is, not from the individual) from any source (and not just a person, organisation or agency), where providing such notice is reasonable.

This would clarify and give certainty to the law in line with the information sheet and guidance issued by the Office. In this regard, there has been a call for the Office’s guidance material to provide greater legal certainty. The Law Council of Australia (36) suggests that the Privacy Act could be amended so that in the context of a matter going before a court, if an organisation has relied upon the Office’s guidance this will be seen by the court as persuasive.

Amending NPP 1.5 would, in effect, bring similar certainty to the Office’s interpretation and regulation of this principle, and would not further impact on current business practice.

**No change**

While this was not a high-profile issue in submissions, it has been a matter of significant discussion between the Office and a range of businesses over past years. Therefore, while one option would be to monitor the issue further, this would mean that a known uncertainty in the law is not resolved in a timely fashion.

---

240 Information Sheet 17-2003: Privacy and Personal Information that is Publicly Available.
9.6 Recommendation: NPP 1.5 – ‘Someone’

The Australian Government should consider amending NPP 1.5 to remove the term ‘someone’, and to make clear that an organisation has an obligation to take reasonable steps to provide notice to an individual when collecting their personal information indirectly, from any source.

9.7 NPP 2 – primary purpose and the collection of health information

Background

NPP 2 regulates the use and disclosure of personal information. It provides that uses or disclosures of personal information are limited to the purpose for which the information was initially collected (the ‘primary purpose’), unless a prescribed exception applies. There are a range of exceptions to this general rule.

The exception at NPP 2.1(a) provides that health information can be used or disclosed for another purpose where this is directly related to the primary purpose and the individual would reasonably expect the use or disclosure.

Law and Policy

Since the introduction of the private sector provisions of the Privacy Act, the Office has interpreted the primary purpose of collecting health information by a health service provider in the health care context as the main or dominant reason the individual is seeking assessment, treatment or care.

There is an intentionally close relationship between the primary purpose and the directly related purpose provisions at NPP 2.1(a), which in this context means that with open communication between a health service provider and an individual (something to be expected in the delivery of quality health care), a holistic approach to care can be agreed either explicitly or implicitly. In other words, where the individual expects their health information to be used in the delivery of health care to them in a holistic manner, it is permissible under NPP 2.

In implementing the NPPs, the Office has noted the health sector’s history of confidentiality; a duty incumbent upon health professionals as part of their fiduciary duty to individuals who are their patients or clients. While privacy obligations are broader than is a health professional’s duty of confidentiality, the latter builds upon the former. In that regard, there is good reason to expect that health professionals, and the services they work in, ought to be...
practised in appropriately managing the information of their patients and in respecting their wishes. The policy underpinning the NPPs anticipates the nature of this special relationship.

Accordingly, to date the Office has considered that the dynamic relationship within NPP 2 between primary purpose, directly-related secondary purposes and the test of meeting the individual’s reasonable expectations seeks to reflect the complex, dynamic and sometimes shifting relationships that patients and health care providers enjoy.

In this manner, the principle can permit a holistic approach to the handling of health information as part of holistic care to most individuals most of the time, and where this is what they expect. However, it also leaves room for negotiation of information-handling within alternate care arrangements for those with this need.

What submissions say - issues

A number of submissions argue against defining the primary purpose of collection on an episodic basis. These submissions suggest that the current understanding of ‘primary purpose’ in the health context is too narrow.

The Mental Health Privacy Coalition (58) submits that:

‘modern health practice favours an approach to healthcare, which is holistic. An holistic approach to healthcare encompasses the idea of taking into account the past experiences and healthcare history of a particular person, and trying to project into the future their likely healthcare needs.’

The Australian Medical Association (29) similarly submits that:

‘the concept of “primary purpose” when applied in the context of health care should accommodate the meaning ‘the health care and well being of the patient’, unless another meaning is specifically agreed to between the doctor and the patient’.

The Australian Medical Association (29) also notes that what constitutes ‘primary purpose’ in a health care context is ‘a critical matter that underlies the whole privacy scheme’ and stated that ‘the care of a patient’s health and well being is not achieved by episodic care.’

Accordingly, there are some calls for NPP 2 to be amended to, as described by the Australian Medical Association, ‘recognise that the “primary purpose” of collection of health information by doctors is the “health care and well being” of the patient.’

---

241 Relevant submissions include the Mental Health Privacy Coalition, 58 and the Australian Medical Association, 29.
One submission notes the change in the health sector to ‘healthcare models such as shared care and hospital at home programmes where services are provided by the public and private health care sectors working cooperatively’, South Australian Department of Health (53). It is suggested that such models lead to consumers assuming that their information is shared.

Where such models of health care result in uses or disclosures directly related to the primary purpose of collection, then they would be permitted by NPP 2.1(a) so long as consumers are aware such exchanges may occur.

**Options for Reform**

**Amend National Privacy Principle 2**

The Australian Government could amend NPP 2 in line with the suggestion of the Australian Medical Association to put beyond doubt that the ‘primary purpose’ of collection of health information by health services is for the holistic health care and well being of the patient.

One effect of such a change could be to allow any organisation that collects health information to use and disclose it for broader purposes, some of which individuals may not expect.

The amendment could somehow seek to constrain the breadth of further uses or disclosures of health information to a clinical, health care context, if this can be suitably defined. Even in this case, however, some individuals (as patients) may lose the ability to negotiate and enforce alternate health information-handling arrangements. Furthermore, it is unclear whether such amendment to the law would eventually reflect on the scope of the duty of confidentiality, as currently interpreted by the courts.

**Broaden interpretation of NPP 2 through guidance**

The Office could engage with the health sector and work to re-interpret and clarify current understanding of the primary purpose of collection of health information in the delivery of a health service. This could involve the Office issuing guidance similar to the scope of the legislative change suggested above, but either as binding or non-binding guidelines.

Under this approach, the Office could offer guidance stating that the collection of health information in the delivery of a health service is always for the provision of holistic health care.

Although not a legislative reform option, the practical effect would be the same, and the concerns noted above would seem to apply; most notably, the application of the principle loses its flexibility in responding to the myriad of relationships between health professionals and their patients.
Further guidance and education

The Office could engage with the health sector in order to develop more guidance to explain the operation of NPP 2.1(a) in the context of delivering health services. For example, that holistic care is permissible under NPP 2 on the grounds that collecting health information for a primary purpose and using it for other (holistic) health care delivery reasons over time (that is, directly related purposes) equates to the delivery of holistic treatment. This would be subject to open communication by providers with individuals about how care is delivered, and the approach to care being within the individual’s reasonable expectations.

In effect, this approach would reflect and refine the Office’s current view that in general, health service providers can proceed to provide care in the manner they consider appropriate for the individual they are treating, having recourse to that person’s needs and views. The provider always needs to take care not to exceed the expectations of the individual. In most situations, an individual's expectations will be apparent through normal communication with their provider.

If a provider is uncertain, they should check whether the individual understands, and whether they expect the proposed use or disclosure of their information. Of course, the provider may choose explicitly to seek consent.

This approach would be broadly consistent with that currently adopted by the Office. However, the Office recognises that more effective guidance is needed to assist health services to understand how NPP 2 can work for them. Furthermore, the Office could work with professional bodies to assist them in reflecting the operation of this key principle, to their members.

9.8 Recommendations: Primary purpose and health information

77 The Office will work with the health sector to develop further guidance about the operation of NPP 2 as it specifically relates to the issue of primary and secondary purpose in health care.

78 The Office will provide clearer guidance on the operation of NPP 2 to give more effective and practical assistance to demonstrate how the principle operates. This will take into account the range of relationships between health services and individuals, particularly where individuals agree to a holistic approach to the delivery of a health service.
9.9 NPP 3

Law and Policy

NPP 3 concerns data quality. It obliges an organisation to take reasonable steps to maintain the quality of the personal information it collects. The Office states in its Guidelines to the National Privacy Principles that ‘the aim of NPP 3 is to prevent the adverse consequences for people that might result from an organisation collecting, using, or disclosing inaccurate, incomplete or out-of-date personal information’.

What submissions say - issues

A small number of submissions commented on the operation of NPP 3. Some comments were also raised in consultations.

Debate focused on whether data quality was intended as an overriding obligation on organisations when considering their personal information-handling practices. Some organisations argued in favour of certain contentious practices on the basis of their need to comply with NPP 3.

A confidential submission states that enabling organisations to use Australian Government identifiers, such as Medicare and passport numbers, means they could better comply with their data quality obligations. A comment made in consultations is that organisations need to be able to use publicly available personal information to ensure data quality and accuracy.

Electronic Frontiers Australia (51) states that NPP 3 is being used by organisations to justify bundled consent practices. The justification is that using a bundled consent approach reduces the amount of data entered into an information system, therefore limiting data entry errors. Electronic Frontiers Australia believes that:

> 'such an interpretation of the NPP 3 accuracy requirement is plainly contrary to the intent and objectives of the (Privacy Act). NPP 3 must be amended to make clear that it cannot be used as an excuse for giving individuals less choice in relation to the use and disclosure of their personal information.'

The Australian Medical Association in consultations argued that data quality is important, but not overriding.

The Consumer Credit Legal Centre (62) and the Consumers’ Federation of Australia (65) contend that a number of the listings given to credit reporting agencies by credit providers are inaccurate. These submissions contend that credit providers can have systematic inaccurate listings, as seen from the

---

242 Electronic Frontiers Australia 51, Consumers’ Federation of Australia 65, Consumer Credit Legal Centre 62 and a confidential submission.
One.Tel listing inaccuracies. The submissions argue that situations such as that involving One.Tel, indicate that adequate systems are not in place to ensure data quality of credit report listings.

**Options for Reform**

**Provide more guidance**

Some organisations seem to consider that their obligation (under NPP 3) to keep personal information accurate, complete and up-to-date is an absolute obligation. Indeed, that it could be used to justify intruding upon an individual’s privacy.

However, obligations under the NPPs are not absolute. NPP 3 requires an organisation to take reasonable steps to ensure data quality. This includes balancing NPP obligations with other obligations and responsibilities.

In the Office’s view, it is not reasonable to take steps under NPP 3 to ensure data accuracy where this does not have any privacy benefit for the individual. For example, an individual may choose deliberately not to tell an organisation that they have changed addresses, because they do not want to be contacted. Unless pursuing a debt or in respect of a similarly serious matter, it is unlikely to be reasonable for the organisation to seek to update the information they hold about the person, just to contact them further.

In this context, the Office could provide further guidance about organisations’ obligations under NPP 3, and the reasonable steps they may need to take to maintain data quality.

**Amend the law**

The Australian Government could amend NPP 3 to seek to clarify that maintaining data quality is not an absolute obligation above all others. However, given the high-level nature of the NPPs that call for judgement by organisations when handling personal information in the particular circumstances at hand, this may not be a preferred approach.

**9.10 Recommendation: NPP 3 - Data quality**

The Office will provide further guidance to organisations about their obligations under NPP 3, particularly to ensure they take a proportional approach to complying with the principle. This will include guidance about organisations taking into account whether or not there are good privacy reasons for seeking to update an individual’s personal information.
9.11  **NPP 4**
All the issues for this NPP are dealt with in Chapter 6.

9.12  **NPP 5**
All the issues for this NPP are dealt with in Chapter 4.

9.13  **NPP 6**
All the issues for this NPP are dealt with in Chapter 4.

9.14  **NPP 7**

**Law and policy**

National Privacy Principle 7 seeks to ensure that the increasing use of Australian Government identifiers\(^{243}\) does not lead to a de facto system of universal identity numbers, and to prevent any loss of privacy from the combination and re-combination of this data, including with other information. Similarly, tax file number legislation already restricts the way an organisation can collect, use or disclose a tax file number.

Unless prescribed by regulation, NPP 7.1 prohibits an organisation from collecting an Australian Government assigned identifier from the people with whom it deals, and then using that identifier to organise and match other personal information with reference to that identifier. In other words, an organisation is not permitted to adopt an Australian Government identity number as if it were its own identity number.

National Privacy Principle 7.2 limits organisations’ handling of Australian Government identifiers. Such identifiers may be used:

- 'where necessary for the organisation to fulfil its obligations to the agency that assigned the identifier to the individual; or
- in certain prescribed circumstances in which there is a public interest, set out as exceptions (e) to (h) for NPP 2. These exceptions include uses or disclosures in the interest of lessening or preventing a serious and imminent threat to any individual, or where the use or disclosure is authorised or required by or under law.'

---

\(^{243}\) An Australian Government identifier is a unique combination of letters and numbers, such as a Medicare number, which Australian Government agencies or their contracted service providers allot to an individual.
NPPs 7.1A and 7.2(c) allow for regulations to be proposed by the Attorney-General, and made by the Governor-General, to relax these restrictions.

**Issues**

The Office is aware of a range of practices involving the collection of Australian Government identifiers for the purpose of establishing adequate evidence of identity (EOI). For example, individuals may be asked to present a Medicare card, a current Australian Passport, a document with a Centrelink customer reference number (CRN), or a citizenship certificate when first entering into a transaction with an organisation. In some cases, organisations take a photocopy of the Medicare card or relevant page of the Passport. Such a photocopy would include the Medicare number or Passport number, which is the identifier in question.

The Office is also aware of increasing concerns relating to identity theft, identity fraud and identity security, which appear to be driving an increase in demands for EOI. This can lead to concerns from individuals about the increasing collection of information from their important identity documents; particularly for transactions in which such EOI was not previously sought.

NPP 7 does not explicitly prohibit the collection of identifiers. However, NPP 1 regulates the collection of personal information generally, and this would include identifiers. Therefore, if an organisation is to collect an identifier it must consider its obligations under NPP 1.

**What the submissions say - issues**

**Government identifiers and concessions**

Telstra (110), the Department of Family and Community Services (81) and Centrelink (107) discuss procedures by which private organisations such as Telstra confirm that an individual is a customer of a relevant Australian Government agency, and so is entitled to a concession rate from the organisation.

One convenient means of doing such a check is for the organisation to collect an individual’s Centrelink CRN, and pass it onto Centrelink to confirm the person’s eligibility to concessional entitlements. However, the restriction on the use or disclosure of Australian Government identifiers (under NPP 7.2) may prohibit this use of the CRN. This would make it more difficult for organisations to confirm a customer’s eligibility for concessional services.

These three submissions suggest that NPP 7 should be amended to include an exception to the limitation upon the use and disclosure of Australian Government identifiers, so that the individual concerned can give consent to the use or disclosure of their identifier.
Identifiers and market research

The Association of Market Research Organisations (AMRO) and the Australian Market and Social Research Society (AMSRS) (61) suggest that NPP 7 has the unintended effect of curtailing practices that pose no threat to privacy and are potentially of significant public benefit. AMRO/AMSRS suggest that conducting a longitudinal study into the effectiveness of a Centrelink program would only be possible with the use of Australian Government identifiers.

Stakeholder meetings also included questions about the meaning and intention of NPP 7.

AMRO/AMSRS suggest that NPP 7 be clarified; preferably involving amendment to enable the use and transfer of Australian Government identifiers by organisations where it would pose no threat to any individual’s privacy. AMRO/AMSRS note that there are technical means of making use of such identifiers which nevertheless do not allow the attribution of any personal information to identified individuals.

Collection of identifiers

Xamax Consultancy Pty Ltd (3) suggests that insufficient protection against the multiple usage of identifiers may give rise to the consolidation of personal information.

In particular, this submission singles out the lack of a prohibition on the collection of Australian Government identifiers. The submission also notes the lack of prohibitions on the handling of state and territory government identifiers, such as driver’s licence numbers.

Options for reform

Consent exception

Allowing the use and disclosure of Australian Government identifiers, with the consent of the individual concerned, may assist both organisations and government agencies to provide services, including concessional services, more efficiently.

However, as discussed further in the section on bundled consent (see Chapter 4) some organisations may seek to make consent to the use and disclosure of identifiers a condition of providing a service, or a condition on providing a service at a concessional rate. The widespread collection of Australian Government identifiers may arise. This would be inconsistent with the policy intention of NPP 7, which is to ensure that Australian Government identifiers do not become de facto national identity numbers, allowing for easy aggregation of personal data across unrelated organisations.
Making regulations

The regulation-making powers under NPP 7, and sub-sections 100(2) and (3), appear to be sufficient to deal with the particular concerns raised in the submissions.

However, the Department of Family and Community Services (81) suggests that making such regulations would be a cumbersome approach to the issue. In considering such an argument, the policy intent underpinning this principle must be borne in mind. This was ‘to prevent the gradual adoption of government identity numbers as de facto universal identity numbers’.\footnote{Privacy Amendment (Private Sector) Bill 2000, Revised Explanatory Memorandum – Parliament of the Commonwealth of Australia: Senate, para 382.}

Therefore, while the impact (for government agencies) in making regulations needs to be acknowledged, this needs to be balanced with the public interest in ensuring that NPP 7 achieves its stated policy aims.

The making of regulations can address the matter raised about checking the concessional status of individuals without risking the widespread collection, use and disclosure of Australian Government identifiers. Similarly, if warranted, a research study that required the use of such identifiers beyond the existing scope of NPP 7.2 could be enabled by regulation.

Prohibit the collection of identifiers

The collection of identifiers into a record is regulated by NPP 1, including NPP 1.1 which limits the collection of personal information to that which is necessary for one or more of an organisation’s functions or activities.

Therefore, if an identifier is collected by an organisation, but cannot be lawfully used or disclosed pursuant to NPP 7.2, then the collection is not necessary for one of the organisation’s functions or activities. As a consequence, the collection would be prohibited by NPP 1.1.

Depending on the circumstances, and where there are no other laws requiring or authorising the collection of the identifier in question, the collection of an identifier ‘just in case’ it is needed for some future purpose is likely to be in breach of NPP 1.1. Arguably, therefore, there is no requirement for an amendment to the principle to specifically prohibit the collection of Australian Government identifiers.

No change

Given the significance of the policy underpinning this principle and the flexibility permitted by regulation-making (to address specific issues requiring the use or disclosure of identifiers), no change in the law may be warranted.
9.15 **Recommendation: NPP 7 - Identifiers**

The Australian Government should consider using the existing regulation-making mechanism under NPP 7 to address circumstances such as those identified by Centrelink regarding concessional entitlements.

9.16 **NPP 8**

All issues for this NPP are dealt with in Chapter 8.

9.17 **NPP 9**

All issues for this NPP are dealt with in Chapter 3.

9.18 **NPP 10 - Collection of Family History Information - Public Interest Determinations 9 and 9A**

**Law and Policy**

Public Interest Determinations (PIDs) enable the Privacy Commissioner to reduce the privacy protections of one or more of the National Privacy Principles (NPPs) in certain circumstances. In order to issue a PID, the Privacy Commissioner must be satisfied of two matters: first, that an act or practice of an organisation breaches or may breach a NPP or a privacy code (a Code); and second, that the act or practice should nevertheless be permitted because the public interest in its continuation substantially outweighs the public interest in adhering to the NPP or the Code.

The Privacy Commissioner issued PIDs 9 and 9A in October 2002. The combined effect of PIDs 9 and 9A is to exempt providers of health services, in certain circumstances, from complying with NPP 10.1.

---

245 The Privacy Commissioner made earlier temporary public interest determinations in similar terms in December 2001 for the commencement of the private sector privacy provisions.

246 Section 6 of the Privacy Act defines ‘health service’ as an activity performed in relation to an individual:

- to assess, record, maintain or improve the individual’s health; or
- to diagnose the individual’s illness or disability; or
- to treat the individual’s illness or disability or suspected illness or disability; or
- the dispensing of a prescription drug or medicinal preparation by a pharmacist.

The Privacy Act applies to all private sector organisations that deliver these types of services including: traditional health service providers such as private hospitals and day surgeries, medical practitioners, pharmacists, and allied health professionals such as counsellors, as well as complementary therapists, gyms, weight loss clinics and many others.
NPP 10.1 limits the collection of sensitive information, by an organisation, from or about an individual without that person's consent. The Commissioner found that the collection of sensitive information about third parties (which is necessary to obtain the family, social or medical history of an individual during the provision of a health service) did not fall within the limited exceptions outlined in NPP 10.1 to 10.3. The Commissioner was of the view that such collection would breach NPP 10.1.

The collection of family, social and medical history information is a critical part of providing assessment, diagnosis and treatment to individuals. The Commissioner acknowledged that obtaining the consent of third parties to collect their information, and notifying those individuals about these collections, would be impractical, inefficient and detrimental to the provision of quality health outcomes.

The Commissioner recognised that the public interest is served by the efficient and accurate diagnosis and treatment of individuals by clinicians, and this is fundamentally underpinned by the taking of family, social and medical histories.

Under PIDs 9 and 9A, a health service provider may collect health information from an individual (a health consumer) about a third party, without the consent of the third party, when both of the following conditions are met:

- 'the collection of the third party's information into an individual's social, family or medical history is necessary to provide a health service directly to the individual; and
- the third party's information is relevant to the family, social or medical history of the individual receiving the health service.'

PIDs 9 and 9A do not represent an exemption from all of the NPPs. Therefore, NPPs 1 to 9 and NPPs 10.2 and 10.3 continue to apply to the handling of this type of information by organisations providing a health service.

In addition, health service providers that collect third party information into social, family or medical histories must comply with their obligations under NPP 2.1(a). Therefore, proposed further uses or disclosures of this information for secondary purposes must be directly-related to the initial reason it was collected (that is, for the history of the individual seeking treatment) and something the third party would reasonably expect; that is unless one of the other exceptions to NPP 2 applies.

The Commissioner issued PIDs 9 and 9A for a period of 5 years, with a review of the Determinations to take place at or before that time (that is, by October 2007).
What the submissions say - issues

A number of submissions comment on the effectiveness and importance of PIDs 9 and 9A. There is a general consensus that the PIDs are necessary and that they are operating smoothly.

Submissions state that the collection of family histories, as allowed by PIDs 9 and 9A, is most important when providing holistic treatment to an individual.

This is particularly so in the area of mental health where it is considered important for the treating clinician to have an understanding of the individual’s perceived familial relationships. A family history narrative will reveal much about the individual’s attitudes and emotional make-up, which is generally more important to the clinician than information about the family members per se (Australian Medical Association 29, Mental Health Privacy Coalition, 58). As mentioned by the Australian Medical Association (29) ‘leaving aside the impracticalities of obtaining third-party consent, should the family member’s consent be required, or should the family member access and correct the information, the value of the collected information would be lost.’

No submissions raised negative views on the operation of PIDs 9 and 9A. Conversely, there is a call for the Privacy Act to be amended to substantively incorporate these PIDs\(^ {247}\). For example, there is concern that the PIDs operate for only a finite time. Given the ongoing nature of this activity (that is, it is an enduring element of providing quality health care), submissions recommend that the PIDs be incorporated into law. This would help assure health service providers that they can continue to offer best practice healthcare, including the collection of social, family and medical history information.

Support for the inclusion of provisions in the Privacy Act to reflect the PIDs came from submissions including the Australian Medical Association (29) the Mental Health Privacy Coalition (58) and the Australian Government Department of Health and Ageing (99).

The Mental Health Privacy Coalition (58) outlines some examples of limited exceptions that may be considered were the PIDs to be incorporated into the Privacy Act. These exceptions include limiting the collection of a third party’s DNA or electronic health record information only with their consent. The Mental Health Privacy Coalition acknowledges that emergency health situations may require variations to such exceptions.

The Office is aware of common practices in the insurance industry pertaining to the collection of family history information when an individual makes an application for some insurance products. In its report *Essentially Yours: The Protection of Human Genetic Information in Australia*, the Australian Law Reform Commission and the Australian Health Ethics Committee note that:

\(^{247}\) See Australian Government Department of Health and Ageing 99, Australian Medical Association 29 and Mental Health Privacy Coalition 58.
insurance companies routinely collect family medical history information and use it in underwriting. The collection and use is based on the long recognised fact that certain diseases have a hereditary component, and that information about the medical history of family members is relevant in assessing the applicant’s risk.\textsuperscript{248}

The Australian Law Reform Commission and the Australian Health Ethics Committee Inquiry received submissions calling for amendments to the Privacy Act, or the issuing of amended PIDs, to provide clarity that the collection of family medical history information, in the course of processing an application for insurance, is not a breach of NPP 10.\textsuperscript{249} The Inquiry recommended (Recommendation 28-3) that a PID be sought by insurers. To date, the Privacy Commissioner has not considered an application for a PID in these terms.

**Options for Reform**

**Amend NPP 10 - add additional exception**

The principle could be amended by inserting an additional exception, such as a NPP 10.1(f). This exception would mirror the operation of the PIDs for the collection of third party information into a family, social or medical history in the delivery of a health service to an individual.

**Amend NPP 10 - add additional provision to NPP 10.2(b)**

As NPP 10.2 provides a specific context for the collection of health information in order to deliver a health service, there may be greater policy cogency in adding a provisions (such as a NPP 10.2(b)(iii)) to reflect the operation of the PIDs.

**Amend NPP 10 with exceptions or variations**

The substance of the PIDs could be incorporated into NPP 10 (for instance in either of the above ways), but with some further exceptions or variations.

For example, the Mental Health Privacy Coalition stated that ‘the Commissioner may wish to delineate some extremely limited exceptions. For instance, it may be appropriate to rule that DNA information offered to a healthcare practitioner, which concerns another individual, even a family member, should only be provided with the specific consent of that family member.’

\textsuperscript{248} Essentially Yours: Insurance and Genetic Privacy, para 28.49 (p. 751)

\textsuperscript{249} Op. cit., paras 28.55 – 28.58 (pp. 752-753)
Consideration could also be given to the views of the insurance sector, as expressed to the Australian Law Reform Commission and the Australian Health Ethics Committee Inquiry into the protection of human genetic information (particularly in regard to Recommendation 28-3). If the collection practices of the insurance sector reflect a similar public interest, and are as settled as those of the health service delivery sector, then for the same reasons a substantive amendment to the law may be more appropriate than a PID.

No change

No amendment is made to the Privacy Act. In this case, the PIDs would need to be reviewed by October 2007. In accordance with the *Legislative Instruments Act 2003*, any further determinations would be operational for a period of up to 10 years. This would not meet the need for regulatory certainty expressed during the Review.

9.19 **Recommendations: NPP 10 - Public Interest Determinations**

81 The Australian Government should consider amending NPP 10 to include an exception that mirrors the operation of Public Interest Determinations 9 and 9A.

82 The Australian Government should consider undertaking consultation on limited exceptions or variations to the collection of family, social and medical history information, particularly with regard to genetic information and the collection practices of the insurance industry.

9.20 **NPP 10.2 - Collecting health information without consent**

**Law and Policy**

**Introduction**

The Privacy Act recognises important social interests that include the effective delivery of health services. In many circumstances, health service providers can only provide individuals with health services after collecting information about the individual and their health. On the other hand, the individual is entitled to retain a degree of control over the collection of their health information and how it is handled.
NPP 10.1(a) prohibits an organisation from collecting an individual’s sensitive information (including their health information) unless they have given consent. There are a number of exceptions to this rule.

Exception: in the delivery of a health service

One such exception (NPP 10.2) recognises the need for a health service provider to collect an individual’s health information in order to deliver health services to them. This is permissible when the information is collected by the provider either as required by law (other than the Privacy Act), or in accordance with rules that are established by competent health or medical bodies which deal with obligations of professional confidentiality; such rules must bind the health service provider (NPP 10.2 (a) (i) and (ii)).

Scope of the exception

The two sub-paragraphs of NPP 10.2 recognise two different circumstances, in the delivery of health services, where the collection of an individual’s health information can be effected without consent.

Firstly, a health service provider may have a legal obligation set out in statute, or arising from the common law, which requires the collection of certain health information in the context of providing a health service. For example, a medical practitioner may need to collect a child’s health information from the child’s parent or guardian, under their duty of care to the child.

Secondly, for example, a professional body of health service providers could establish a set of rules, or a binding code of practice, which (in the context of the body’s commitment to observing confidentiality) also includes binding rules relating to the collection of health information from and about individuals.

Purpose of the exception

In broad terms, NPP 10.2 aims to enable organisations providing health services to collect individuals’ health information without consent, subject to certain conditions. The principle attempts to achieve a workable balance between therapeutic need and individuals’ privacy rights.

The issue

While not significantly reflected in submissions, the Office’s experience with NPP 10.2 raises issues of interpretation and application of the law.

Required by law

NPP 10.1 (b) allows sensitive information (which includes health information) to be collected without consent where ‘the collection is required by law’. This provision appears to repeat, in part, the wording of NPP 10.2 (b)(ii).
However, the relationship between NPPs 10.1 (b) and 10.2 (b)(i) is not clear. It is difficult to distinguish between the limitations upon organisations generally when collecting sensitive information (as required by law) under NPP 10.1(b), and those created by the similarly stated provision (10.2(b)(i)) that are imposed upon organisations delivering health services.

**Authorised by law**

The disclosure of an individual’s health information by a health service provider (or other organisation) without the individual’s consent is permitted under NPP 2.1(g) where such a disclosure is ‘required or authorised by or under law’.

Whereas the more restrictive provisions of NPP 10.2(b)(i), especially in the context of health service delivery, have the potential to unduly impede the effective delivery of such services. The restrictive character of this sub-paragraph may be inconsistent with the Privacy Act’s general reliance upon the ethical traditions, including recognition of the duty of confidentiality, of health service providers.

There may be an argument for recognising that where an organisation is delivering a health service and there is a stated legal authority for it to collect health information about an individual, NPP 10 should permit this to occur without consent.

**Binding rules of confidentiality**

The Privacy Act and the NPPs acknowledge that health professionals have a history of adhering to their duty of confidentiality toward patients and their health information.

This is reflected in provisions such as NPP 10.2(b)(ii), with its reliance upon binding rules of professional bodies that appear to need to pertain to the collection of health information. The exact nature and construction of these binding rules is uncertain given the current construction of the provision.

To date, the Office has not been presented with an example of binding rules that would satisfy the requirements of NPP 10.2(b)(ii), nor is the Office aware of the operation of such rules in the health sector.

**Options for Reform**

**No change**

As the construction and operation of these provisions did not feature generally in submissions or views put to this Review, it may be feasible to take no action on these issues.
Greater clarity through legislative amendment

Given the intent of NPP 10.2, there appears to be merit in providing greater clarity and certainty in the legislative scheme regarding the collection of health information in the delivery of health services, and particularly with regard to the provision of clinical or therapeutic care.

Changes to the legislation could better and more effectively reflect the health sector’s history of working within the duty of confidentiality to patients. This could include permitting the collection of health information (by an organisation when delivering a health service to an individual) when authorised by law, as well as when required by law.

Greater legislative clarity could be provided about the precise nature of the types of binding rules envisaged by NPP 10.2(b)(ii), and particularly to establish (or otherwise) that these rules must deal with matters about the collection of health information (albeit in the context of obligations of professional confidentiality).

With appropriate amendments to NPP 10.2, the balance between the privacy protection afforded to individuals and the need for effective delivery of health services can be better achieved. Further guidance from the Office would be necessary, following such amendments, to assist organisations and the sector in the application of the provisions in practice.

9.21 Recommendations:  NPP 10.2(b)

83 The Australian Government should consider amending NPP 10.2 to permit the collection of health information (under NPP 10.2(b)(i)) ‘as authorised by law’ in addition to ‘as required by law’.

84 The Australian Government should consider amending NPP 10.2(b) (ii) to clarify the nature of the binding rules intended to be covered by this provision, particularly with regard to the substantive content of such rules.
10 Other issues with the private sector provisions of the Privacy Act

10.1 Information of deceased persons

Law and Policy

Privacy Act

The Privacy Act does not appear to create privacy obligations in relation to the handling of personal information of deceased persons. The Privacy Act regulates the handling of ‘personal information’. Personal information is defined under section 6(1) as:

‘information or an opinion (including information or an opinion forming part of a database), whether true or not, and whether recorded in a material form or not, about an individual whose identity is apparent, or can reasonably be ascertained, from the information or opinion;’

The term ‘individual’ is defined under section 6(1) as meaning ‘a natural person’. The term ‘natural person’ is not defined under the Privacy Act or the Acts Interpretation Act 1901; however it appears the term is usually used to distinguish human beings from artificial persons or corporations250. Whether the term ‘natural persons’ includes a deceased human being does not appear to have been subject to judicial consideration in Australia or the United Kingdom. The Office considers the term ‘natural person’ to mean a living human being as this is the plain English meaning of the term.

To add further weight to this view, the legislation does not appear to provide any mechanism for a person to make a complaint other than the individual whose privacy has been interfered with251. Section 36(1) of Privacy Act states:

‘an individual may complain to the Privacy Commissioner about an act or practice that may be an interference with the privacy of the individual’.

250 See Pharmaceutical Society v London and Provincial Supply Association (1879-80) 5 App Cas 857 (‘Pharmaceutical Society’) per Lord Blackburn at 869; see also the definition of ‘individual’ contained in subsection 22(1)(aa) of the Acts Interpretation Act 1901, the object of which is to distinguish between ‘a natural person as opposed to a body corporate or body politic’ (clause 127 of the Explanatory Memorandum to the Law and Justice Legislation Amendment Bill 1990); and also Osborn’s Concise Law Dictionary (7th ed) at 228).

251 Unless, perhaps the decease person’s information falls part of a representative complaint, see sections 36(2) and 38(3).
Therefore, it appears another person could not lodge a complaint about an alleged breach of privacy of a deceased person.

This position can be contrasted with other Commonwealth and state legislation that protects a person’s information generally for thirty years after their death.

**Other State and Commonwealth Legislation**

Some other legislation governing the handling of personal information does protect that information for a period after a person’s death.

Under section 5(3)(a) of the Health Records and Information Privacy Act 2000 (NSW) and section 4(3) of the Privacy and Personal Information Protection Act 1998 (NSW), the definition of personal information does not include information about an individual that has been dead for more than 30 years.

Similarly, ‘personal information’ is defined under section 3(1) of the Victorian Health Records Act 2001 as

‘information or an opinion (including information or an opinion forming part of a database), whether true or not, and whether recorded in a material form or not, about an individual whose identity is apparent, or can reasonably be ascertained, from the information or opinion, but does not include information about an individual who has been dead for more than 30 years;’ (emphasis added).

In Tasmania, the Personal Information Protection Act 2004 was passed in November 2004 and received Royal Assent on 17 December 2004. This legislation applies to deceased persons’ information for 25 years after death.

The draft National Health Privacy Code would apply to the health information of those who have been dead for 30 years or less.

The Freedom of Information Act 1982 under section 41(1), makes specific reference to the protection of a deceased person’s information in relation to the unreasonable disclosure of personal information252.

Also, 30 years is the point for commencement of the ‘open access period’ in section 3(7) of the Archives Act 1983.

**What submissions say - issues**

A small number of submissions refer to the handling of deceased persons’ information. Of those that comment, all recommend that the Privacy Act be

---

252 A document is an exempt document if its disclosure under this Act would involve the unreasonable disclosure of personal information about any person (including a deceased person).
amended to include protection of deceased persons’ information\(^{253}\), with most suggesting the protection be extended to thirty years after a person’s death. This recommendation was made by the Australian Law Reform Commission and the Australian Health Ethics Committee in its report *Essentially Yours: The Protection of Human Genetic Information in Australia* (Recommendation 7-6). In support of recommending that people’s health information be protected for 30 years after their death, the report states that:

> ‘it is desirable that information privacy protection extend to genetic information about deceased individuals because of the implications that the collection, use or disclosure of this information may have for living genetic relatives. It appears preferable for representatives of the deceased to be able to consent to the collection, use or disclosure rather than to leave decisions about these matters outside the Privacy Act’\(^{254}\).

Some submissions recommend (as do the Australian Law Reform Commission and the Australian Health Ethics Committee) that the Privacy Act also be amended to include provisions for decision-making in respect of the personal information of deceased persons, either by a next-of-kin or an authorised person of deceased individuals\(^{255}\). No practical recommendations are made in the submissions, although it is assumed that such amendments would need to include the ability to make a complaint on behalf of the deceased person and to gain access to the deceased person’s information.

**Options for Reform**

**Extend coverage of the Privacy Act to cover the personal information of individuals until 30 years after death**

As discussed above, some Commonwealth and state legislation protects an individual’s personal information for up to 30 years after death. Extending coverage in the Privacy Act in similar terms would bring it in line with such legislation and create greater national consistency.

From consultations it is clear there is considerable confusion among the community about whether or not the Privacy Act covers personal information of people who have died. The policy rationale for protecting all of the personal information of individuals for 30 years after death is unclear.

\(^{253}\) Australian Law Reform Commission 33, National Health and Medical Research Council 32, Australian Privacy Foundation 90, Australian Government Department Health and Ageing 99.

\(^{254}\) *Essentially Yours*, paragraph 7.90.

\(^{255}\) Australian Law Reform Commission 33, National Health and Medical Research Council 32.
Taking this approach could create difficulties for those collecting information for archival purposes after people die, particularly if the collection includes sensitive information, as the person would be unable to consent. Also, there are presently no provisions in the Privacy Act for a person to complain on behalf of a person who has died. Any amendments to the Privacy Act would need to take these issues into account.

**Extend coverage of the Privacy Act to cover the genetic information of individuals until 30 years after death**

The Australian Law Reform Commission and the Australian Health Ethics Committee recommend that the Privacy Act be amended to cover an individual’s genetic information for 30 years after they die.

As stated above, this is because the handling of genetic information of a deceased person can have an impact on their genetic relatives.

However, this matter is outside the terms of reference of this review.

**Consider protection for the information of deceased persons as part of a wider review of the Privacy Act**

There may need to be more consideration of the policy rationale for covering personal information generally, for up to 30 years after a person has died. Also, with possible implications for the construction of the NPPs and other aspects of the legislation, whether the coverage of the Privacy Act should be extended in this regard might be canvassed better in a wider review of the legislation as proposed in recommendation 1.

**10.2 Recommendations: Deceased persons**

85 If the National Health Privacy Code is adopted into the Privacy Act (see recommendation 13), then protection for health information under these provisions would extend to deceased persons. Also, the Australian Government’s response to the Australian Law Reform Commission and the Australian Health Ethics Committee’s Inquiry into the protection of human genetic information in Australia may have implications for the Privacy Act. In addition, the Australian Government should consider as part of a wider review (recommendation 1) whether the jurisdiction of the Privacy Act should be extended to cover the personal information of deceased persons.
10.3 Employee Records Exemption

Law and Policy

Under section 7B(3), an act done, or practice engaged in, by an organisation that is or was an employer of an individual is exempt from the NPPs if the act or practice is directly related to:

- a current or former employment relationship between the employer and the individual and
- an employee record held by the organisation and relating to the individual.

What submissions say

Despite the Terms of Reference expressly excluding the employee records exemption from the Review, a number of submissions comment on the exemption. The issue also arose in consultation sessions.

National Consistency

A goal of the NPPs was to create a single, comprehensive nationally consistent privacy scheme for the private sector. Most of the submissions that raise the employee records exemption do so in the context of examining how the Privacy Act is achieving national consistency.

A concern arising out of submissions is that various pieces of state legislation are being enacted in order to deal with employment privacy issues such as workplace surveillance. This concern was raised in submissions that were both in favour, and against, the exemption.

10.4 Political Exemption

Law and Policy

The exemption for political acts and practices is in section 7C of the Privacy Act. Section 7C(1) states:

An act done, or practice engaged in, by an organisation (the political representative) consisting of a member of a Parliament, or a councillor (however described) of a local government authority, is exempt for the

---

256 For example Consumers' Federation of Australia 65, Australian Information Industry Association Ltd 43, Australian Consumers Association 15, Microsoft Australia 20, Coles Myer Ltd 60, Australian Retailers Association 111, Australian Privacy Foundation 90, Australian Law Reform Commission 33.

257 Microsoft Australia 20, Australian Consumers Association 15, Australian Information Industry Association Ltd 43, Australian Privacy Foundation 90.
purposes of paragraph 7(1)(ee) if the act is done, or the practice is engaged in, for any purpose in connection with:

- an election under an electoral law or
- a referendum under a law of the Commonwealth or a law of a state or territory or
- the participation by the political representative in another aspect of the political process.

Subsections 7C(2), (3) and (4) extend the exemption to contractors, subcontractors and volunteers for registered political parties.

**What submissions say**

A number of submissions comment on the political exemption\(^\text{258}\) despite the exemption being outside the Terms of Reference for the Review. The issue also arose in consultation sessions.

In general, those that did comment upon the exemption did not approve of the exemption.

Also, there is some criticism that the exemption has been excluded from the Terms of Reference of the Review.

---

\(^{258}\) See for example, Australian Privacy Foundation 90, Australian Medical Association 29, Mental Health Privacy Coalition 58.
Appendix 1

Terms of Reference

Review of the Private Sector Provisions of the Privacy Act 1988

I, PHILIP RUDDOCK, Attorney-General of Australia, under section 27(1)(f) of the Privacy Act 1988, request that the Privacy Commissioner review the operation of the private sector provisions contained in the Privacy Amendment (Private Sector) Act 2000 and report on that review not later than 31 March 2005.

In undertaking the review, I ask that the Privacy Commissioner consider the degree to which the private sector provisions meet their objects, being:

a. to establish a single comprehensive national scheme providing, through codes adopted by private sector organisations and National Privacy Principles, for the appropriate collection, holding, use, correction, disclosure and transfer of personal information by those organisations; and

b. to do so in a way that:
   i. meets international concerns and Australia’s international obligations relating to privacy;
   ii. recognises individuals’ interests in protecting their privacy; and
   iii. recognises important human rights and social interests that compete with privacy, including the general desirability of a free flow of information (through the media and otherwise) and the right of business to achieve its objectives efficiently.

Recognising that certain aspects of the private sector provisions are currently, or have recently substantively been, the subject of separate review, the Privacy Commissioner exclude review of:

- genetic information;
- employee records;
- children’s privacy; and
- electoral roll information, and the related exemption for political acts and practices

13 August 2004
# Appendix 2

## Review of the Private Sector Provisions

### Review Reference Group

<table>
<thead>
<tr>
<th>Name</th>
<th>Organisation/Institution</th>
</tr>
</thead>
<tbody>
<tr>
<td>Catherine Bergin</td>
<td>Pharmacy Guild</td>
</tr>
<tr>
<td>Charles Britton</td>
<td>Australian Consumers’ Association</td>
</tr>
<tr>
<td>Pamela Burton</td>
<td>Australian Medical Association</td>
</tr>
<tr>
<td>David Cains and David Kemp</td>
<td>Institute of Mercantile Agents</td>
</tr>
<tr>
<td>Roger Clarke</td>
<td>Xamax Consultancy Pty Ltd</td>
</tr>
<tr>
<td>Chris Connolly</td>
<td>Galexia Consulting</td>
</tr>
<tr>
<td>Peter Coroneos</td>
<td>Internet Industry Association</td>
</tr>
<tr>
<td>Karen Cox</td>
<td>Consumer Credit Legal Centre</td>
</tr>
<tr>
<td>Jeremy Douglas-Stewart</td>
<td>Privacy Law Consulting Australia</td>
</tr>
<tr>
<td>Roger Du Blêt</td>
<td>Small Business Coalition</td>
</tr>
<tr>
<td>Rob Durie</td>
<td>Australian Information Industry Association</td>
</tr>
<tr>
<td>Rob Edwards</td>
<td>Australian Direct Marketing Association</td>
</tr>
<tr>
<td>Greg Evans</td>
<td>Australian Chamber of Commerce and Industry</td>
</tr>
<tr>
<td>Chad Gates</td>
<td>Australian Retailers Association, Victoria</td>
</tr>
<tr>
<td>Ian Gilbert</td>
<td>Australian Bankers' Association</td>
</tr>
<tr>
<td>Duncan Giles</td>
<td>Freehills</td>
</tr>
<tr>
<td>Dr William Glasson</td>
<td>Australian Medical Association</td>
</tr>
<tr>
<td>Helen Gordon</td>
<td>Australian Finance Conference</td>
</tr>
<tr>
<td>Irene Graham</td>
<td>Electronic Frontiers Australia</td>
</tr>
<tr>
<td>Graham Greenleaf</td>
<td>University of New South Wales</td>
</tr>
<tr>
<td>Ron Hardaker</td>
<td>Australian Finance Conference</td>
</tr>
<tr>
<td>Helen Hopkins</td>
<td>Consumers Health Forum of Australia Inc</td>
</tr>
<tr>
<td>Graeme Innes</td>
<td>Human Rights and Equal Opportunity Commission</td>
</tr>
<tr>
<td>Rebecca Johnstone</td>
<td>Insurance Council of Australia</td>
</tr>
<tr>
<td>Katherine Lane</td>
<td>Consumer Credit Legal Centre</td>
</tr>
<tr>
<td>Lindsay B. May</td>
<td>Fundraising Institute of Australia Ltd</td>
</tr>
<tr>
<td>Mike McGrath</td>
<td>Department of Health and Ageing</td>
</tr>
<tr>
<td></td>
<td>Investment and Financial Services Association (IFSA)</td>
</tr>
<tr>
<td>David Mico</td>
<td>Australian Market &amp; Social Research Society</td>
</tr>
<tr>
<td>Julia Nesbitt</td>
<td>Australian Medical Association</td>
</tr>
<tr>
<td>Michael Pickering</td>
<td>Telstra Corporation</td>
</tr>
<tr>
<td>Suzanne Pigdon</td>
<td>Coles Myer Ltd</td>
</tr>
<tr>
<td>Jodie Sangster</td>
<td>Australian Direct Marketing Association</td>
</tr>
<tr>
<td>Joan Sheedy</td>
<td>Attorney-General's Department</td>
</tr>
<tr>
<td>John Sergeant</td>
<td>Association of Market Research Organisations</td>
</tr>
<tr>
<td>Name</td>
<td>Organization</td>
</tr>
<tr>
<td>-----------------------</td>
<td>---------------------------------------------------</td>
</tr>
<tr>
<td>Lindy Smith</td>
<td>Privacy Management Pty Ltd</td>
</tr>
<tr>
<td>Bryan Stevens</td>
<td>Real Estate Institute of Australia</td>
</tr>
<tr>
<td>Melissa Stratton</td>
<td>Baycorp Advantage</td>
</tr>
<tr>
<td>Dr Michael Tatchell</td>
<td>Pharmacy Guild</td>
</tr>
<tr>
<td>Dr Laga Van Beek</td>
<td>Department of Health and Ageing</td>
</tr>
<tr>
<td>Alison Verhoeven</td>
<td>Real Estate Institute of Australia</td>
</tr>
<tr>
<td>Dr Sue-Anne Wallace</td>
<td>Fundraising Institute of Australia Ltd</td>
</tr>
<tr>
<td>Sarah Ward</td>
<td>Coles Myer Ltd</td>
</tr>
<tr>
<td>Nigel Waters</td>
<td>Australian Privacy Foundation</td>
</tr>
<tr>
<td></td>
<td>Pacific Privacy Consulting</td>
</tr>
<tr>
<td></td>
<td>Privacy Law &amp; Policy Reporter</td>
</tr>
<tr>
<td>Burchell Wilson</td>
<td>Australian Chamber of Commerce and Industry</td>
</tr>
<tr>
<td>Angela Dally</td>
<td>Coles Myer Ltd</td>
</tr>
<tr>
<td>Melanie King</td>
<td>Australian Retailers Association NSW</td>
</tr>
<tr>
<td>Scott McClellan</td>
<td>Australian Direct Marketing Association</td>
</tr>
</tbody>
</table>
Appendix 3

Submissions Received

1 Human Research Ethics Committee, University of Western Australia
2 Australian Hotels Association
3 Xamax Consultancy Pty Ltd
4 Multicultural Australia
5 Restaurant and Catering Australia
6 Private individual – confidential
7 Private individual
8 Australian Business and Specialist Publishers – confidential
9 Aged Psychiatry Service, The Geelong Hospital
10 Private Health Insurance Ombudsman
11 Not for profit organisation (name withheld)
12 Comcare
13 Real Estate Institute of Australia
14 National Credit Union Association Inc
15 Australian Consumers Association (ACA)
16 Australian Compliance Institute
17 Australian Wine Selectors – confidential
18 Allianz Australia Insurance Ltd – confidential
19 Australian Broadcasting Authority
20 Microsoft Australia
21 Private Individual
22 Australian Chamber of Commerce and Industry
23 Tenants Union of Victoria
24 Royal Institute for Deaf and Blind Children
25 Insolvency and Trustee Service Australia
26 Virgin Mobile (Australia) Pty Ltd
27 Office of the Health Services Commissioner
28 Department of Public Health, The University of Adelaide
29 Australian Medical Association
30 Australasian Epidemiology Association
31 Private Individual – confidential
32 National Health and Medical Research Council
33 Australian Law Reform Commission
34 Promina Group Limited
35 Suncorp-Metway Ltd
36 Law Council of Australia – Business Law Section
37 Australian Physiotherapy Association
38 Australian Institute of Private Detectives
39 Australasian Federation of Family History Organisations Inc
40 ANZ
41 MDA national Insurance Pty Ltd – confidential
42 Private individual – confidential
43 Australian Information Industry Association
44 Cerebral Palsy League of Queensland
45 The Australian Industry Group – confidential
46 Free TV Australia
47 Professor Graham Greenleaf
48 Comvice Pty Ltd
49 Private Hospitals Association of Qld – confidential
50 Dun & Bradstreet (Australia) Ltd – confidential
51 Electronic Frontiers Australia Inc
52 Fundraising Institute-Australia Ltd
53 Department of Health (SA), Corporate Resources
54 Australian Federation of AIDS Organisations (AFAO)
55 Telethon Institute for Child Health Research
56 Banking and Financial Services Ombudsman Limited; Insurance Ombudsman Service Limited; Financial Industry Complaints Service; Telecommunications Industry Ombudsman; Energy and Water Ombudsman (Victoria)
57 Confidential
58 Mental Health Privacy Coalition
59 Insurance Council of Australia Ltd
60 Coles Myer Limited
61 Association of market research Organisations (AMRO) and the Australian Market and Social Research Society (AMSRS)
62 Consumer Credit Legal Centre (NSW) Inc
63 Australian Finance Conference
64 Credit Union Services Corporation (CUSCAL)
65 Consumers’ Federation of Australia (CFA)
66 Privacy Law Consulting Australia (PLCA)
67 Australian Direct Marketing Association
68 Scope
69 Tenants Union of Queensland Inc
70 Australian Bankers’ Association
71 Acxiom Australia
72 Communications Law Centre
73 Private Individual
74 The Salvation Army Australia Southern Territorial Headquarters
75 Clubs Australia & New Zealand
76 Australian Health Insurance Association – confidential
77 Chamber of Commerce & Industry of WA (Inc)
78 Royal District Nursing Service
79 The Mailing House
80 Australian Private Hospitals Association
81 Department of Family and Community Services
82 Dr Gillian Hall, national Centre for Epidemiology and Population Health
83 Commerce Queensland
84 Sensis
85 Financial Planning Association of Australia
86 Baycorp Advantage
87 Tenants Union ACT
88 Confidential
89 Investment and Financial Services Association Ltd
90 Australian Privacy Foundation
<table>
<thead>
<tr>
<th></th>
<th>Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>91</td>
<td>Australian Association of Permanent Building Societies – confidential</td>
</tr>
<tr>
<td>92</td>
<td>Business SA</td>
</tr>
<tr>
<td>93</td>
<td>The Pharmacy Guild of Australia</td>
</tr>
<tr>
<td>94</td>
<td>Australian Communications Authority</td>
</tr>
<tr>
<td>95</td>
<td>Department of Health (SA), Office of the Chief Executive</td>
</tr>
<tr>
<td>96</td>
<td>Clubs Queensland – confidential</td>
</tr>
<tr>
<td>97</td>
<td>St John Ambulance Australia (Australian Office)</td>
</tr>
<tr>
<td>98</td>
<td>Optus</td>
</tr>
<tr>
<td>99</td>
<td>Department of Health and Ageing</td>
</tr>
<tr>
<td>100</td>
<td>Australian Institute of Health and Welfare</td>
</tr>
<tr>
<td>101</td>
<td>Department of Health, Western Australia</td>
</tr>
<tr>
<td>102</td>
<td>eBay Australia and New Zealand</td>
</tr>
<tr>
<td>103</td>
<td>The Australian Psychological Society Ltd</td>
</tr>
<tr>
<td>104</td>
<td>Opera Australia</td>
</tr>
<tr>
<td>105</td>
<td>FCS Online</td>
</tr>
<tr>
<td>106</td>
<td>Housing Industry Association</td>
</tr>
<tr>
<td>107</td>
<td>Centrelink</td>
</tr>
<tr>
<td>108</td>
<td>ACT Health – confidential</td>
</tr>
<tr>
<td>109</td>
<td>Australia Post</td>
</tr>
<tr>
<td>110</td>
<td>Telstra Corporation Limited</td>
</tr>
<tr>
<td>111</td>
<td>Australian Retailers Association</td>
</tr>
<tr>
<td>112</td>
<td>Vodafone Australia Limited</td>
</tr>
<tr>
<td>113</td>
<td>Victorian Automobile Chamber of Commerce</td>
</tr>
<tr>
<td>114</td>
<td>Australian Guardianship and Administration Committee</td>
</tr>
<tr>
<td>115</td>
<td>Australian Collectors Association, Institute of Mercantile Agents,</td>
</tr>
<tr>
<td></td>
<td>Australian Institute of Credit Management</td>
</tr>
<tr>
<td>116</td>
<td>The Police Association</td>
</tr>
<tr>
<td>117</td>
<td>St Vincent de Paul Society, National Council</td>
</tr>
<tr>
<td>118</td>
<td>Private Individual – confidential</td>
</tr>
<tr>
<td>119</td>
<td>Australian Academy of Science</td>
</tr>
<tr>
<td>120</td>
<td>Australian Crime Commission</td>
</tr>
<tr>
<td>121</td>
<td>Submission received - confidential</td>
</tr>
<tr>
<td>122</td>
<td>Submission received – confidential</td>
</tr>
<tr>
<td>123</td>
<td>Collection House Limited</td>
</tr>
<tr>
<td>124</td>
<td>Australian Press Council</td>
</tr>
<tr>
<td>125</td>
<td>Queensland Retail Traders &amp; Shopkeepers Association</td>
</tr>
<tr>
<td>126</td>
<td>Australian Securities and Investments Commission – confidential</td>
</tr>
<tr>
<td>127</td>
<td>Australian Nursing Federation</td>
</tr>
<tr>
<td>128</td>
<td>Australian Competition &amp; Consumer Commission</td>
</tr>
<tr>
<td>129</td>
<td>Australian Federal Police</td>
</tr>
<tr>
<td>130</td>
<td>Private Individual</td>
</tr>
<tr>
<td>131</td>
<td>Mortgage Industry Association of Australia</td>
</tr>
<tr>
<td>132</td>
<td>Legacy Co-ordinating Council Inc</td>
</tr>
<tr>
<td>133</td>
<td>Queensland Government</td>
</tr>
<tr>
<td>134</td>
<td>Australian Electoral Commission</td>
</tr>
<tr>
<td>135</td>
<td>Private Individual</td>
</tr>
<tr>
<td>136</td>
<td>NSW Police Legal Services</td>
</tr>
</tbody>
</table>
Appendix 4

National Privacy Principles

The National Privacy Principles as set out in Schedule 3 of the Privacy Act 1988 are as follows:

1 Collection

1.1 An organisation must not collect personal information unless the information is necessary for one or more of its functions or activities.

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

1.3 At or before the time (or, if that is not practicable, as soon as practicable after) an organisation collects personal information about an individual from the individual, the organisation must take reasonable steps to ensure that the individual is aware of:

(a) the identity of the organisation and how to contact it; and

(b) the fact that he or she is able to gain access to the information; and

(c) the purposes for which the information is collected; and

(d) the organisations (or the types of organisations) to which the organisation usually discloses information of that kind; and

(e) any law that requires the particular information to be collected; and

(f) the main consequences (if any) for the individual if all or part of the information is not provided.

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

1.5 If an organisation collects personal information about an individual from someone else, it must take reasonable steps to ensure that the individual is or has been made aware of the matters listed in subclause 1.3 except to the extent that making the individual aware of the matters would pose a serious threat to the life or health of any individual.
2 Use and disclosure

2.1 An organisation must not use or disclose personal information about an individual for a purpose (the secondary purpose) other than the primary purpose of collection 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;

(ii) the individual would reasonably expect the organisation to use or disclose the information for the secondary purpose; or

(b) the individual has consented to the use or disclosure; or

(c) if the information is not sensitive information and the use of the information is for the secondary purpose of direct marketing:

(i) it is impracticable for the organisation to seek the individual’s consent before that particular use; and

(ii) the organisation will not charge the individual for giving effect to a request by the individual to the organisation not to receive direct marketing communications; and

(iii) the individual has not made a request to the organisation not to receive direct marketing communications; and

(iv) in each direct marketing communication with the individual, the organisation draws to the individual’s attention, or prominently displays a notice, that he or she may express a wish not to receive any further direct marketing communications; and

(v) each written direct marketing communication by the organisation with the individual (up to and including the communication that involves the use) sets out the organisation’s business address and telephone number and, if the communication with the individual is made by fax, telex or other electronic means, a number or address at which the organisation can be directly contacted electronically; or
(d) if the information is health information and the use or disclosure is necessary for research, or the compilation or analysis of statistics, relevant to public health or public safety:

(i) it is impracticable for the organisation to seek the individual’s consent before the use or disclosure; and

(ii) the use or disclosure is conducted in accordance with guidelines approved by the Commissioner under section 95A for the purposes of this subparagraph; and

(iii) in the case of disclosure – the organisation reasonably believes that the recipient of the health information will not disclose the health information, or personal information derived from the health information; or

(e) the organisation reasonably believes that the use or disclosure is necessary to lessen or prevent:

(i) a serious and imminent threat to an individual’s life, health or safety; or

(ii) a serious threat to public health or public safety; or

(f) the 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; or

(g) the use or disclosure is required or authorised by or under law; or

(h) the organisation reasonably believes that the use or disclosure is reasonably necessary for one or more of the following by or on behalf of an enforcement body:

(i) the prevention, detection, investigation, prosecution or punishment of criminal offences, breaches of a law imposing a penalty or sanction or breaches of a prescribed law;

(ii) the enforcement of laws relating to the confiscation of the proceeds of crime;

(iii) the protection of the public revenue;

(iv) the prevention, detection, investigation or remedying of seriously improper conduct or prescribed conduct;
(v) the preparation for, or conduct of, proceedings before any court or tribunal, or implementation of the orders of a court or tribunal.

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 2.1 does not override any existing legal obligations not to disclose personal information. Nothing in subclause 2.1 requires an organisation to disclose personal information; an organisation is always entitled not to disclose personal information in the absence of a legal obligation to disclose it.

Note 3: An organisation is also subject to the requirements of National Privacy Principle 9 if it transfers personal information to a person in a foreign country.

2.2 If an organisation uses or discloses personal information under paragraph 2.1(h), it must make a written note of the use or disclosure.

2.3 Subclause 2.1 operates in relation to 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.

2.4 Despite subclause 2.1, an organisation that provides a health service to an individual may disclose health information about the individual to a person who is responsible for the individual if:

(a) the individual:

   (i) is physically or legally incapable of giving consent to the disclosure; or

   (ii) physically cannot communicate consent to the disclosure; and

(b) a natural person (the carer) providing the health service for the organisation is satisfied that either:

   (i) the disclosure is necessary to provide appropriate care or treatment of the individual; or

   (ii) the disclosure is made for compassionate reasons; and

(c) the disclosure is not contrary to any wish:
(i) expressed by the individual before the individual became unable to give or communicate consent; and

(ii) of which the carer is aware, or of which the carer could reasonably be expected to be aware; and

(d) the disclosure is limited to the extent reasonable and necessary for a purpose mentioned in paragraph (b).

2.5 For the purposes of subclause 2.4, a person is responsible for an individual if the person is:

(a) a parent of the individual; or

(b) a child or sibling of the individual and at least 18 years old; or

(c) a spouse or de facto spouse of the individual; or

(d) a relative of the individual, at least 18 years old and a member of the individual’s household; or

(e) a guardian of the individual; or

(f) exercising an enduring power of attorney granted by the individual that is exercisable in relation to decisions about the individual’s health; or

(g) a person who has an intimate personal relationship with the individual; or

(h) a person nominated by the individual to be contacted in case of emergency.

2.6 In subclause 2.5:

*child* of an individual includes an adopted child, a step-child and a foster-child, of the individual.

*parent* of an individual includes a step-parent, adoptive parent and a foster-parent, of the individual.

*relative* of an individual means a grandparent, grandchild, uncle, aunt, nephew or niece, of the individual.

*sibling* of an individual includes a half-brother, half-sister, adoptive brother, adoptive sister, step-brother, step-sister, foster-brother and foster-sister, of the individual.
3 **Data quality**

An organisation must take reasonable steps to make sure that the personal information it collects, uses or discloses is accurate, complete and up-to-date.

4 **Data security**

4.1 An organisation must take reasonable steps to protect the personal information it holds from misuse and loss and from unauthorised access, modification or disclosure.

4.2 An organisation must 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 National Privacy Principle 2.

5 **Openness**

5.1 An organisation must set out in a document clearly expressed policies on its management of personal information. The organisation must make the document available to anyone who asks for it.

5.2 On request by a person, an organisation must take reasonable steps to let the person know, generally, what sort of personal information it holds, for what purposes, and how it collects, holds, uses and discloses that information.

6 **Access and correction**

6.1 If an organisation holds personal information about an individual, it must provide the individual with access to the information on request by the individual, except to the extent that:

   (a) in the case of personal information other than health information – providing access would pose a serious and imminent threat to the life or health of any individual; or

   (b) in the case of health information – providing access would pose a serious threat to the life or health of any individual; or

   (c) providing access would have an unreasonable impact upon the privacy of other individuals; or

   (d) the request for access is frivolous or vexatious; or
(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; or

(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; or

(g) providing access would be unlawful; or

(h) denying access is required or authorised by or under law; or

(i) providing access would be likely to prejudice an investigation of possible unlawful activity; or

(j) providing access would be likely to prejudice:

(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; or

(ii) the enforcement of laws relating to the confiscation of the proceeds of crime; or

(iii) the protection of the public revenue; or

(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 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.

6.2 However, where providing access would reveal evaluative information generated within the organisation in connection with a commercially sensitive decision-making process, the organisation may give the individual an explanation for the commercially sensitive decision rather than direct access to the information.
Note: 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.

6.3 If the organisation is not required to provide the individual with access to the information because of one or more of paragraphs 6.1(a) to (k) (inclusive), the organisation must, if reasonable, consider whether the use of mutually agreed intermediaries would allow sufficient access to meet the needs of both parties.

6.4 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.

6.5 If an organisation holds personal information about an individual and the individual is able to establish that the information is not accurate, complete and up-to-date, the organisation must take reasonable steps to correct the information so that it is accurate, complete and up-to-date.

6.6 If the individual and the organisation disagree about whether the information is accurate, complete and up-to-date, and the individual asks the organisation to associate with the information a statement claiming that the information is not accurate, complete or up-to-date, the organisation must take reasonable steps to do so.

6.7 An organisation must provide reasons for denial of access or a refusal to correct personal information.

7 Identifiers

7.1 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; or

(b) an agent of an agency acting in its capacity as agent; or

(c) a contracted service provider for a Commonwealth contract acting in its capacity as contracted service provider for that contract.

7.1A However, subclause 7.1 does not apply to the adoption by a prescribed organisation of a prescribed identifier in prescribed circumstances.
7.2 An organisation must not use or disclose an identifier assigned to an individual by an agency, or by an agent or contracted service provider mentioned in subclause 7.1, unless:

(a) the use or disclosure is necessary for the organisation to fulfil its obligations to the agency; or

(b) one or more of paragraphs 2.1(e) to 2.1(h) (inclusive) apply to the use or disclosure; or

(c) the use or disclosure is by a prescribed organisation of a prescribed identifier in prescribed circumstances.

Note: There are prerequisites that must be satisfied before the matters mentioned in paragraph (c) are prescribed: see subsection 100(2).

7.3 In this clause:

*identifier* includes a number assigned by an organisation to an individual to identify uniquely the individual for the purposes of the organisation’s operations. However, an individual’s name or ABN (as defined in the *A New Tax System (Australian Business Number) Act 1999*) is not an *identifier*.

8 **Anonymity**

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

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

(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.

10 Sensitive information

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 nonprofit 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.

10.2 Despite subclause 10.1, an organisation may collect health information about an individual if:

(a) the information is necessary to provide a health service to the individual; and

(b) the information is collected:

(i) as required by law (other than this Act); or

(ii) in accordance with rules established by competent health or medical bodies that deal with obligations of professional confidentiality which bind the organisation.

10.3 Despite subclause 10.1, an organisation may collect health information about an individual if:

(a) the collection is necessary for any of the following purposes:

(i) research relevant to public health or public safety;

(ii) the compilation or analysis of statistics relevant to public health or public safety;

(iii) the management, funding or monitoring of a health service; and

(b) that 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; and

(c) it is impracticable for the organisation to seek the individual’s consent to the collection; and

(d) the information is collected:
(i) as required by law (other than this Act); or

(ii) in accordance with rules established by competent health or medical bodies that deal with obligations of professional confidentiality which bind the organisation; or

(iii) in accordance with guidelines approved by the Commissioner under section 95A for the purposes of this subparagraph.

10.4 If an organisation collects health information about an individual in accordance with subclause 10.3, the organisation must take reasonable steps to permanently de-identify the information before the organisation discloses it.

10.5 In this clause:

*non-profit organisation* means a non-profit organisation that has only racial, ethnic, political, religious, philosophical, professional, trade, or trade union aims.
Appendix 5

Information Privacy Principles

The Information Privacy Principles as set out in s.14 of the Privacy Act 1988 are as follows:

**Principle 1**

**Manner and purpose of collection of personal information**

1. Personal information shall not be collected by a collector for inclusion in a record or in a generally available publication unless:
   
   (a) the information is collected for a purpose that is a lawful purpose directly related to a function or activity of the collector; and
   
   (b) the collection of the information is necessary for or directly related to that purpose.

2. Personal information shall not be collected by a collector by unlawful or unfair means.

**Principle 2**

**Solicitation of personal information from individual concerned**

Where:

(a) a collector collects personal information for inclusion in a record or in a generally available publication; and

(b) the information is solicited by the collector from the individual concerned;

the collector shall take such steps (if any) as are, in the circumstances, reasonable to ensure that, before the information is collected or, if that is not practicable, as soon as practicable after the information is collected, the individual concerned is generally aware of:

(c) the purpose for which the information is being collected;

(d) if the collection of the information is authorised or required by or under law – the fact that the collection of the information is so authorised or required; and
(e) any person to whom, or any body or agency to which, it is the collector’s usual practice to disclose personal information of the kind so collected, and (if known by the collector) any person to whom, or any body or agency to which, it is the usual practice of that first-mentioned person, body or agency to pass on that information.

**Principle 3**

**Solicitation of personal information generally**

Where:

(a) a collector collects personal information for inclusion in a record or in a generally available publication; and

(b) the information is solicited by the collector;

the collector shall take such steps (if any) as are, in the circumstances, reasonable to ensure that, having regard to the purpose for which the information is collected:

(c) the information collected is relevant to that purpose and is up to date and complete; and

(d) the collection of the information does not intrude to an unreasonable extent upon the personal affairs of the individual concerned.

**Principle 4**

**Storage and security of personal information**

A record-keeper who has possession or control of a record that contains personal information shall ensure:

(a) that the record is protected, by such security safeguards as it is reasonable in the circumstances to take, against loss, against unauthorised access, use, modification or disclosure, and against other misuse; and

(b) that if it is necessary for the record to be given to a person in connection with the provision of a service to the record-keeper, everything reasonably within the power of the record-keeper is done to prevent unauthorised use or disclosure of information contained in the record.
Principle 5

Information relating to records kept by record-keeper

1. A record-keeper who has possession or control of records that contain personal information shall, subject to clause 2 of this Principle, take such steps as are, in the circumstances, reasonable to enable any person to ascertain:

   (a) whether the record-keeper has possession or control of any records that contain personal information; and

   (b) if the record-keeper has possession or control of a record that contains such information:

      (i) the nature of that information;

      (ii) the main purposes for which that information is used; and

      (iii) the steps that the person should take if the person wishes to obtain access to the record.

2. A record-keeper is not required under clause 1 of this Principle to give a person information if the record-keeper is required or authorised to refuse to give that information to the person under the applicable provisions of any law of the Commonwealth that provides for access by persons to documents.

3. A record-keeper shall maintain a record setting out:

   (a) the nature of the records of personal information kept by or on behalf of the record-keeper;

   (b) the purpose for which each type of record is kept;

   (c) the classes of individuals about whom records are kept;

   (d) the period for which each type of record is kept;

   (e) the persons who are entitled to have access to personal information contained in the records and the conditions under which they are entitled to have that access; and

   (f) the steps that should be taken by persons wishing to obtain access to that information.

4. A record-keeper shall:
(a) make the record maintained under clause 3 of this Principle available for inspection by members of the public; and

(b) give the Commissioner, in the month of June in each year, a copy of the record so maintained.

**Principle 6**

**Access to records containing personal information**

Where a record-keeper has possession or control of a record that contains personal information, the individual concerned shall be entitled to have access to that record, except to the extent that the record-keeper is required or authorised to refuse to provide the individual with access to that record under the applicable provisions of any law of the Commonwealth that provides for access by persons to documents.

**Principle 7**

**Alteration of records containing personal information**

1. A record-keeper who has possession or control of a record that contains personal information shall take such steps (if any), by way of making appropriate corrections, deletions and additions as are, in the circumstances, reasonable to ensure that the record:

(a) is accurate; and

(b) is, having regard to the purpose for which the information was collected or is to be used and to any purpose that is directly related to that purpose, relevant, up to date, complete and not misleading.

2. The obligation imposed on a record-keeper by clause 1 is subject to any applicable limitation in a law of the Commonwealth that provides a right to require the correction or amendment of documents.

3. Where:

(a) the record-keeper of a record containing personal information is not willing to amend that record, by making a correction, deletion or addition, in accordance with a request by the individual concerned; and

(b) no decision or recommendation to the effect that the record should be amended wholly or partly in accordance with that
request has been made under the applicable provisions of a law of the Commonwealth;
the record-keeper shall, if so requested by the individual concerned, take such steps (if any) as are reasonable in the circumstances to attach to the record any statement provided by that individual of the correction, deletion or addition sought.

**Principle 8**

**Record-keeper to check accuracy etc. of personal information before use**

A record-keeper who has possession or control of a record that contains personal information shall not use that information without taking such steps (if any) as are, in the circumstances, reasonable to ensure that, having regard to the purpose for which the information is proposed to be used, the information is accurate, up to date and complete.

**Principle 9**

**Personal information to be used only for relevant purposes**

A record-keeper who has possession or control of a record that contains personal information shall not use the information except for a purpose to which the information is relevant.

**Principle 10**

**Limits on use of personal information**

1. A record-keeper who has possession or control of a record that contains personal information that was obtained for a particular purpose shall not use the information for any other purpose unless:

   (a) the individual concerned has consented to use of the information for that other purpose;

   (b) the record-keeper believes on reasonable grounds that use of the information for that other purpose is necessary to prevent or lessen a serious and imminent threat to the life or health of the individual concerned or another person;

   (c) use of the information for that other purpose is required or authorised by or under law;
(d) use of the information for that other purpose is reasonably necessary for enforcement of the criminal law or of a law imposing a pecuniary penalty, or for the protection of the public revenue; or

(e) the purpose for which the information is used is directly related to the purpose for which the information was obtained.

2. Where personal information is used for enforcement of the criminal law or of a law imposing a pecuniary penalty, or for the protection of the public revenue, the record-keeper shall include in the record containing that information a note of that use.

**Principle 11**

**Limits on disclosure of personal information**

1. A record-keeper who has possession or control of a record that contains personal information shall not disclose the information to a person, body or agency (other than the individual concerned) unless:

   (a) the individual concerned is reasonably likely to have been aware, or made aware under Principle 2, that information of that kind is usually passed to that person, body or agency;

   (b) the individual concerned has consented to the disclosure;

   (c) the record-keeper believes on reasonable grounds that the disclosure is necessary to prevent or lessen a serious and imminent threat to the life or health of the individual concerned or of another person;

   (d) the disclosure is required or authorised by or under law; or

   (e) the disclosure is reasonably necessary for the enforcement of the criminal law or of a law imposing a pecuniary penalty, or for the protection of the public revenue.

2. Where personal information is disclosed for the purposes of enforcement of the criminal law or of a law imposing a pecuniary penalty, or for the purpose of the protection of the public revenue, the record-keeper shall include in the record containing that information a note of the disclosure.

3. A person, body or agency to whom personal information is disclosed under clause 1 of this Principle shall not use or disclose the information for a purpose other than the purpose for which the information was given to the person, body or agency.
Appendix 6

Community Attitudes towards Privacy 2004

This survey was conducted by Roy Morgan Research in May 2004. The objectives of the research were to:

- Identify current privacy behaviour
- Identify community expectations about privacy
- Identify perceptions and beliefs about appropriate levels of privacy
- Gauge levels of knowledge about privacy
- Gauge levels of knowledge about privacy laws and the OFPC
- Find any shifts in these perceptions to get information about the impact of the Office’s activities or the Privacy Act.

Knowledge of privacy rights

- The number of respondents who say they have adequate knowledge has increased from 2001 (18%) to 26% in 2004
- But levels are still low – only one in four people surveyed claimed adequate knowledge of privacy rights. 38% of people know very little or nothing about their privacy rights, although this figure has decreased from 52% in 2001
- In the 2001 study, 52% of the younger respondents (18-24) claimed to know very little about their rights. By 2004, this had reduced to 36%, which is not significantly different to the rest of the population 18+.

Level of knowledge of privacy

- 53% of respondents knew that government agencies are covered by privacy law though 26% of people thought that they were not and 21% of respondents did not know
- 56% of people know that banks, insurance companies and other financial institutions are covered by privacy law (while 29% think not and 14% do not know)
- 47% of respondents knew that there are some restrictions on charities, private schools and private hospital and other NGOs (while 32% think not and 21% did not know)
- Males have higher level of knowledge about the coverage of government departments by the Privacy Act
- Respondents with more education were more likely to have higher level of knowledge about the coverage of the Privacy Act.

This research indicates that there is still a great deal of misunderstanding amongst half the population about privacy laws.
Awareness of Privacy Commissioner

- There has been little change in awareness of Federal Privacy Commissioner between 2001 (36%) and 2004 (34%)
- Males have a higher awareness (40%) than females (28%)
- The lowest levels of awareness are among 18 – 24 year olds (26%)
- BUT only 7% of respondents would report the misuse of information to the Federal or State Privacy Commissioner. 19% of respondents said they would report it to the ombudsman, 15% would report it to the organisation involved, 13% would report it to the Police, 10% would report it to the local consumer affairs office and 8% of respondents said that they would report it to their local or state MP
- However, there has been a steady increase in awareness about the Federal privacy Commissioner from 1994 where 2% reported that they would report misuse of personal information to the Office to 2001 where the figure rose to 5% to 2004 where it hit 7%.

These figures indicate that even if respondents know about the Office, they do not know what the Office’s role is.

Trust in organisations

Levels of trust have increased in some organisations between 2001 and 2004 including:

- Health service providers
- Financial organisations
- Market research companies
- Government organisations
- Retailers
- Real estate agents

BUT not internet sales companies

Overall, health service providers are the most trusted organisations, followed by financial organisations, government organisations, charities, retailers, market research orgs, real estates with the last being internet organisations.

There has been little change in mean levels of trustworthiness between 2001 and 2004.

Perceptions of invasions of privacy

- Still high levels of people (approximately 90-95%) regard the following as invasions of privacy:
  - Business gets hold of personal information
  - Business monitors internet activity without permission
  - Business uses personal info for alternate purpose
Business asks for irrelevant personal info
- But asking for ID is not regarded by most as an invasion of privacy
- 38% of respondents reported that there had been an increase in incidence of asking for ID, while the majority 56% claimed it was about the same and 4% claimed there was a decrease.

**Reluctance to provide personal information**

The studies in 2001 and 2004 show reluctance to provide similar kinds of personal information including:

- Financial information – bank accounts/ income information is by far and away the most sensitive information which people are reticent to disclose
- Contact details – especially phone number
- Health information.

Reasons for reluctance include an increase in concern about crime and a desire to avoid being sent unsolicited material.

**Protective behaviours**

Compared with the 2001 survey the 2004 research indicated mixed results about awareness of privacy issues. Respondents in 2004 were more likely to leave information off forms, but less likely to refuse to deal with an organisation.

**Marketing material, the electoral roll and the white pages**

The number of people who totally disagreed with use of the Electoral Roll for marketing has increased by 7% from 70% to 77%.

The number of people who totally disagree with use of white pages has stayed the same (46%). The number of people who agree has increased from 42% to 44%.

**Trade off between privacy and customer service**

According to the research the most important elements of a privacy policy were:

- How the information will be used (this was by far the most important information included in a privacy policy)
- If and when the information will be passed on
- What information will be kept.

**Government departments and privacy**

Unique identifier for ID purposes and to access government services on the internet:
• 53% of people were in favour of a unique identifier for these purposes, though 41% of people were against this idea
• Males favoured the idea of a government identifier more than women
• Respondents on higher incomes were more in favour of a government identifier than respondents on lower income.

Circumstances under which government departments should be able to share information

• The majority of respondents agree that government departments should be able to share information, but only in some circumstances
• Only 9% of people said that departments should be able to share information under any circumstances, while 24% of people said not under any circumstances
• Males (11%) were more likely agree to sharing under any circumstances than women (8%)
• People on lower incomes were more likely to say that government departments should not share information under any circumstances (27%)
• People over 50 (13%) were more likely to agree to sharing under any circumstances, than younger people (4%).

Purposes for which government departments should be able to share information most often cited were (in order of frequency) to:

• Prevent crime
• Update information
• Improve efficiency – lowest.

Health services

Attitudes towards Doctors discussing medial details with other health professionals without consent if they thought that it would assist treatment

• Slight increase in people being comfortable with doctors discussing health info with other doctors if would help health outcome from 53% in to 2001 to 60% in 2004
• Males are more likely to be comfortable with this than females
• Older people are more likely to be comfortable with this than younger people
• Respondents with less education were more likely to assent to this than people with higher education.

Attitudes towards a health number to enable the government to better track the use of Health Services:

• 57% of respondents agreed to a health number to track services including 28% who strongly agreed
• 36% of people disagree with this idea while 4% are undecided
• Males, young people and older people are more likely to agree.

Slightly more people agree with the idea of a health number (57%) than a government number (53%).

**Inclusion in health database**

• 64% of people think inclusion should be voluntary compared to 66% in 2001
• 32% of people think that inclusion should be a matter of course (compared to 28% in 2001)
• Males (35%), and older people (37%) were more likely to think inclusion should be a matter of course

**Permission for use of de-identified health information for Research**

• 64% of people think that permission should be sought
• 33% of respondents think that permission is not necessary
• Females (68%) were more likely to think that permissions should be sought than males (59%)
• 18 – 24 year olds most likely to think permission should be sought (71%)
• People with less education were more likely to think that permission should be sought.

**Privacy in the Workplace**

Respondent views were polarized on the issue of reading Work emails:

• One quarter (23%) of respondents think employers should be able to read emails
• One third (34%) think employers should not have this right.

Males (26%) more likely to agree with employers reading work emails than females (19%) and respondents over 35 (25%) years of age were more likely to agree with this than 18-34 year olds (16%).

Views on employers using surveillance equipment and monitoring devices that track what employees type are similar with roughly one quarter agreeing with the use of these surveillance techniques and one third disagreeing.

There was more concern about the monitoring of telephone conversations by employers:

• Only 5% of people thought it was acceptable for employers to do this whenever they choose though 35% of people agreed with it for quality of service purposes
• 59% of respondents said that employee drug testing should only be conducted when it is necessary to ensure safety
• 83% of respondents stated that a workplace privacy policy is important to have.

**Internet usage**

65% of respondents use the internet once a week or more (up from 51% in 2001).

The level of concern about security of personal information when dealing over the internet has risen since 2001 from 57% to 62% in 2004.

More people are reading privacy policies in 2004 (67%) than in 2001 (55%):

• The people who said they had adequate amount of privacy knowledge are more likely to read privacy policies
• However, those who said they had more concerns about security were no more likely to read privacy policy than those with fewer concerns
• Reading a privacy policy online made 14% of people more comfortable and secure whereas in 2001 it assuaged the fears of 18% of respondents.

Other findings from the survey about online behaviour include that:

• 3 in 10 give false information online. Younger people are more likely to do this than older people
• 80% of people regularly update antivirus software
• 49% use a firewall
• 48% have at some stage rejected cookies
• 47% use a spam filter
• 38% use temporary email accounts
• 28% use software to protect anonymity.
Appendix 7

Information Sheet 13:

2001 The Privacy Commissioner’s Approach to Promoting Compliance with the Privacy Act

Ensuring that organisations comply with their obligations under the Privacy Act is one of the Office’s most important functions. Good advice and good rules only make a real difference if they are put into practice. This information sheet sets out the approach the Office intends to take to promoting compliance with the requirements of the Privacy Act and the mechanisms the Act provides to accomplish this objective.

Privacy solutions

Our Strategic Plan, launched in March 2000, explicitly states that the primary value we seek to deliver to our stakeholders stems from developing privacy solutions that build confidence throughout the Australian community. In implementing the new provisions in the Privacy Act, the Office will be seeking to find privacy solutions that deliver good privacy protection for individual Australians while imposing no undue burdens on the organisations involved.

Advice and assistance in preference to punishment

The Office takes the approach that compliance will be achieved most often by helping organisations to comply rather than seeking out and punishing the few organisations that do not. The large majority of Australian organisations in the private sector wish to comply with their legal obligations. The Office’s emphasis will be on providing advice, assistance and information. This is our first and preferred approach at all times. Our experience indicates that such an approach will be all that is necessary to resolve the large majority of matters that come to our attention. Nevertheless, when breaches of the Act are identified they will be actively pursued. The Office will take care to ensure that breaches of the Act are remedied and complainants’ concerns addressed, including through compensation where that is warranted.

Investigating and resolving complaints

In line with this focus, the Office’s approach to handling complaints is one which aims at achieving fair and workable outcomes for the parties involved. In summary, our process is based on taking the following steps:
• When we receive a complaint, we first check if the parties have attempted to resolve their differences directly and, if not, whether it would be appropriate for them to try. For private sector organisations covered by the National Privacy Principles or an approved code under Part IIIAA of the Act, this is mandated by section 40(1A) of the Act. In other words, we encourage internal complaints handling at the organisational level as a first step.

• If this fails, we enter a stage of conciliation based on accepted principles of alternative dispute resolution. In most cases, we rely on phone calls and letters to the parties. In a small proportion of more intractable matters, we may meet with the parties face to face.

• This process has been very successful in the established areas of the Commissioner’s jurisdiction, which cover Commonwealth government agencies, tax file numbers, spent convictions and the consumer credit reporting industry. Most complaints are closed under section 41(2)(a) on the grounds that the respondent has adequately dealt with the matter rather than by the Commissioner issuing a formal determination.

• In the large majority of complaints over the last five years, resolution has involved measures other than monetary compensation. Only around six per cent of complaints have involved financial compensation. In all but a few serious matters, the amounts have been between $500 and $3,000.

• The Commissioner has the power to make a formal determination in relation to complaints (s.52). A determination may prohibit the respondent organisation from continuing or repeating conduct that has breached the Act. It may direct the organisation to perform any reasonable course of conduct to redress loss or damage suffered by the complainant. It may direct the organisation to pay a specified amount to the complainant by way of compensation. However, in the last 12 years, successive Commissioners have found it necessary to use the formal determination making power under s.52 in only two cases.

• If the parties do not comply with the terms of a determination, s.55A of the Act allows us to approach the Federal Court or the Federal Magistrates Court to seek enforcement via a new (de novo) hearing. So far, the Office has never needed to take this step.

Commissioner-initiated investigations

The Office will take the same approach in relation to investigations that the Commissioner conducts on his or her own initiative.

The Privacy Act (s.40(2)) gives the Commissioner the power to carry out an investigation without having received a complaint. This power is available if there may have been an interference with privacy and the Commissioner thinks it is desirable that the matter be investigated. This power may be used where there appears to be a serious breach of privacy that has strong public interest implications. Whether the Office has received complaints about the organisation in the past is also a factor.

The first approach in these cases is to write to the organisation asking for further information. If there then appears to have been a breach of the Act, the
action the Office takes will depend upon the respondent’s acknowledgment of the breach and its preparedness to take appropriate remedial action.

**Injunctions**

The Commissioner has powers under s.98 of the Act to seek an injunction from the Federal Court to ensure compliance with the Act. An injunction may prohibit an organisation from engaging in conduct that would breach the Act or require it to take steps to bring itself into compliance with the Act. An injunction may be sought in relation to a complaint investigation or an own initiative investigation. Again, successive Commissioners have not sought any injunctions so far and this step would be taken only when other more informal means have failed to yield a satisfactory outcome.

**Reporting to the public**

The Office includes in its annual report some cases studies on complaints it has handled and investigations it has carried out. These are reported in summary form and do not generally identify the complainant or respondent. With the new private sector provisions, the Office plans to add to this approach by publishing more frequent, de-identified case notes on complaints it has handled. The aim of these will be to help organisations and the community understand the way the Office applies the provisions of the Act and, where relevant, the provisions of approved codes. On occasion there may be some merit in making public the circumstances of a particular complaint or investigation. This may be, for example, where there is already publicity around a particular matter before it reaches the Office or where, despite all the other approaches the Office has taken, an organisation continues to engage in behaviour that constitutes an interference with privacy. This would clearly be a serious step which could have commercial consequences for the organisation concerned. It would only be appropriate in rare circumstances. In the ordinary course of events, the Commissioner would not consider such a step unless:

- an organisation either repeatedly or very seriously breaches the Privacy Act
- the organisation demonstrates by its actions that it does not intend to comply with its legal obligations, and
- all other measures have failed to change the organisation’s behaviour.

**We will signal our intentions**

The Office will not take action in relation to an organisation without first giving it fair warning of our intentions. Our objective is to assist organisations to comply with their obligations under the Act. Openness and predictability are important means of accomplishing this objective.
We will take measures proportional with the seriousness of the issues

The strength of the measures the Office takes in relation to a particular matter will be proportional to its seriousness. The Office will not be taking strong measures in relation to minor breaches of the law. However, in the most serious matters, the Office will be prepared to use any mechanism available under the Act to achieve an acceptable privacy outcome.

In assessing the seriousness of any particular matter the Office will consider:

- the number of individuals involved
- what disadvantage they have suffered
- whether the matter raises ongoing systemic issues, or is a one-off incident, and
- the willingness of the organisation to take action to resolve the matter and to prevent recurrence - in assessing this, the organisation’s track record in privacy matters will be taken into account.

About Information Sheets

Information sheets are advisory only and are not legally binding. (The NPPs in Schedule 3 of the Privacy Act 1988 (Cth) (the Privacy Act) do legally bind organisations.)

Information sheets are based on the Office’s understanding of how the Privacy Act works. They provide explanations of some of the terms used in the NPPs and good practice or compliance tips. They are intended to help organisations apply the NPPs in ordinary circumstances. Organisations may need to seek separate legal advice on the application of the Privacy Act to their particular situation.

Nothing in an information sheet limits the Privacy Commissioner’s freedom to investigate complaints under the Privacy Act or to apply the NPPs in the way that seems most appropriate to the facts of the case being dealt with.

Organisations may also wish to consult the Commissioner’s guidelines and other information sheets.
Appendix 8

Summary of complaint handling provisions, including powers to investigate

Complaints under the Privacy Act

Individuals who believe that their personal information has been interfered with in some way may complain to the Privacy Commissioner. The complaint may be against an organisation or an agency and must be made in accordance with section 36 of the Act. Individuals cannot complain to the Privacy Commissioner about organisations that are bound by an approved privacy code except where the Commissioner is the adjudicator for that code. However, individuals may ask the Commissioner to review a determination made by a code adjudicator (section 18BI). Representative complaints may also be lodged and accepted by the Office in relation to a privacy issue that affects two or more complainants.

A complaint must be in writing. The Office must provide appropriate assistance to people who require assistance to formulate their complaint. The complaint should specify the respondent that is the subject of the complaint, as well as specify what the act or practice of the agency or organisation was, or may continue to be, that allegedly breaches the Act. These requirements are outlined in Section 36 of the Act. Additionally, Section 38 describes the conditions required for a representative complaint to be made under the Act.

Individuals must first complain the respondent

Generally speaking the Commissioner will not investigate a complaint unless the individual has first complained to the organisation. The Commissioner has the discretion to waive this requirement, however, if it would not be appropriate for the individual to approach the respondent. This might include circumstances where the person responsible for the privacy breach would also investigate the complaint or where there is potential harm to the individual.

Preliminary Enquiry before an investigation

The Office conducts preliminary enquiries where it is not clear whether the Commissioner should investigate a complaint, for example because the organisation concerned may not be within jurisdiction.
A preliminary enquiry is an initial fact-finding exercise conducted by the Office. Section 42 gives the Office the power to contact the respondent named in the complaint in order to gather general information about the respondent in order to, for example, determine whether it may be exempt under the Act. It is not automatic that the complainant’s identity would need to be made known to the respondent in order for the Office to be able to at least partly progress the complaint in the preliminary enquiry stage.

**Deciding not to investigate**

The Act provides a number grounds on which the Commissioner may decide not to investigate, or not to investigate further, a complaint. The grounds are set out in section 41 and include where the complainant has known about the matter for over 12 months, where it is evident that there is no interference with privacy, or where the matter is better dealt with under another law.

The Office looks at the circumstances of the complaint before deciding whether to exercise discretion not to investigate. For example, where the individual has known about the complaint for over 12 months, the Commissioner may still investigate if the complainant can demonstrate some good reason for the delay and the respondent has suffered no prejudice as a result of the delay.

**Investigating complaints**

The Office may investigate a complaint under section 40(1) of the Act if:

- it is about an act or practice may be an interference with the privacy of an individual
- the complaint is against an organisation or agency and
- a complaint has been lodged with the Office in accordance with section 36.

Section 16E states that acts or practices that may be an interference with the privacy of an individual, but appear to have been committed by another individual acting in a private capacity, are not covered by the Act.

The Office has a backlog of complaints awaiting investigation. Complaints (preliminary enquiries and investigations) that do not meet the criteria for an urgent investigation are a queue according to date of receipt.

A complaint may be investigated urgently in limited circumstances. These include:

- where it appears that the complainant is currently suffering significant disadvantage as a result of the events described in the complaint, and the disadvantage is likely to be eliminated, or substantially diminished, by prompt resolution of the complaint
Office of the Privacy Commissioner

- where it appears that the complainant will suffer future significant disadvantage unless the complaint is resolved promptly
- where the complaint appears to raise systemic issues that affect a large number of individuals or
- where the incident complained of is particularly serious and the circumstances suggest that delay in investigation will substantially reduce the probability of obtaining an appropriate resolution.

Under section 40(2) of the Act, the Office may decide it is desirable to investigate possible interferences with privacy where there is no individual complaint. The Office calls such investigations ‘own motion investigations’ (OMI). An OMI may be launched as a result of information that has come to the Office, for example, via published media stories or information provided by an individual who wishes to remain anonymous.

**Conducting investigations**

The Act requires the Commissioner and staff to only disclose information that has come into their possession in the course of their duties. As well, the Commissioner and staff of the Office cannot be compelled to furnish information acquired by them as a consequence of them performing the duties prescribed under the Act, except for the circumstances outlined in the Act (section 96).

Section 43(2) of the Act provides that investigations should be conducted ‘in private’ but otherwise the Commissioner has discretion as to the manner in which any investigation it commences may be conducted.

Generally speaking, in the interests of procedural fairness, parties to the complaint will have access to any information that the Office is considering. However, the Office will consider requests from the complainant or respondent that the information they have provided, or intend to provide, to the Office remain confidential. The Office will firstly seek to discuss this request with either party where it may appear that a resolution of the complaint could be substantially affected by the request. It is worth noting that the Office’s ability to investigate a complaint, and to achieve a satisfactory resolution, may be significantly hampered by a party to the complaint insisting that their submission remain ‘in confidence’.

The Commissioner has the power to compel a person to provide information or documentation as part of the investigation into an alleged interference with an individual’s privacy. The person may be required to provide the required information or documentation in writing, or in person (section 44).

The Commissioner may authorise staff, with the organisation’s consent or under a warrant issued by a Magistrate, to enter the premises of an organisation which is the subject of an investigation or in relation to which enforcement of a determination is sought (section 68).
The Office must also provide parties likely to be adversely affected by a determination with reasonable opportunity to appear before the Commissioner before a finding under section 52 of the Act is made. Under section 43(5) of the Act, the Commissioner may only make a determination after the complainant or respondent has been provided with the opportunity to appear before the Commissioner and to make submissions, orally, in writing or both. Apart from this there is no general obligation on the Office to allow parties to appear before the Commissioner.

A complainant will often have a specific remedy in mind in relation to the complaint made against the agency or organisation. The Office uses the process of statutory conciliation with the aim of negotiating remedies for the complaint in question.

The Office’s role is to provide impartial assistance to both parties to reach a resolution of a complaint. In the process of conciliation the parties may come to any resolution that is acceptable to both.

Where a complaint cannot be resolved by conciliation and the Commissioner makes a determination, the remedies available to the Commissioner are broadly prescribed under section 52 of the Act. They include, for example, a finding that compensation is payable to the complainant.

Possible outcomes of an investigation

Before a final decision in relation to a complaint, the Office will arrive at a preliminary view about the complaint, and provide this view in writing to the parties involved in the complaint for their comment before the final decision is made. A preliminary view is essentially a draft decision about the complaint under consideration and provides both parties with a right of rebuttal in relation to the evidence that the decision has been based on.

A preliminary view may be issued prior to, or after, conciliation between the parties involved in the complaint has been attempted.

A determination is a legal decision or finding made by the Commissioner, as a consequence of which the Act’s enforcement powers are activated (sections 52-62 of the Act). The determination may dismiss the complaint, or find that the complaint has been substantiated and make declarations about action needed, including that conduct should cease or not be repeated, the nature of redress and compensation, or that no further action is needed.

Particular complaints made to the Office may fall under the jurisdiction of a Privacy Code that has been given prior approval by the Commissioner. As such, any investigation of that complaint is carried out by the complaint handling body (independent adjudicator) established for that particular Code, which also has the same determinative powers as the Commissioner does under Section 52 of the Act (section 18BB(3)). As noted earlier, this Office may also act as the final adjudicator in relation to a complaint.
Enforcement refers to the steps as outlined in the Act by which the Commissioner seeks a respondent’s adherence to the determination that the Commissioner has made in respect of the privacy complaint made against that respondent (sections 54-62).

Other matters

Injunctions may be sought through the Federal Court or Federal Magistrate’s Court by the Commissioner or any other person against a person who has engaged, or is proposing to engage in any conduct that constituted, or could constitute, a contravention of the Act (section 98).
Appendix 9

Complaints Statistics

The Office of the Privacy Commissioner has received a total of 3575 complaints since the introduction of the private sector provisions in the Privacy Act (21 December 2001 – 31 January 2005). Of these complaints, 2358 (66%) concerned the National Privacy Principles (NPPs) in the Act.

The number of complaints received by financial year has increased significantly over this period from 194 complaints received in the 2000-2001 financial year to 1276 complaints received in 2003-2004.

This increase can be largely attributed to the rapid growth in the number of complaints received concerning the NPPs since December 2001. The following graph, showing complaints received by jurisdictional area, clearly illustrates this increase:
Complaints Closed

Over the review period (21 December 2001 – 31 January 2005), the Office closed 3137 complaints compared with 3575 complaints received.

Whilst the Office has received more complaints that it has closed since 21 December 2001, the Office has kept pace with the growth in the number of complaints received, as shown in the following graph:

![Complaints Received and Closed By Financial Year](image)

Complaint Outcomes

Section 41 of the Act outlines circumstances in which the Commissioner or her delegates can decide not to investigate, or not investigate further, complaints received under the Act. In most cases, complaints received by the Office are declined or finalised using these powers. In a very small number of cases the Commissioner has finalised a complaint by making a determination under section 52 of the Act.
The following graph shows the grounds by which complaints made under the private sector provisions (NPP complaints) were closed by the Office. This includes NPP complaints that were declined without investigation as well as NPP complaints that were investigated or where preliminary enquiries were conducted.

As shown in the previous graph, 24% of NPP complaints were closed on the grounds that the matter did not fall within the jurisdiction of the Office. Of these complaints, 48.6% were closed due to the application of the exemptions to the NPPs. The following graph shows the breakdown of this general “Not within jurisdiction” category, and illustrates the operation of the exemptions under the Act.
Complaints by Issue Type

The issues raised in complaints tend to cluster around a few of the privacy principles, in particular, the principles dealing with collection (NPPs 1 & 10), disclosure (NPP 2) and access (NPP 6).

The following graph shows the number of NPP complaints received according to issue type (it should be noted that complaints may be recorded under more than one issue type).

![Complaints Received By Issue Type](image)

Whilst this graph shows the issues most likely to arise in complaints received by the Office, it does not necessarily follow that these issues are most recurrent in cases where the Commissioner assesses that there may have be a breach of the Act.

The Commissioner may close a complaint under section 41(2)(a) of the Act, where the Commissioner is satisfied that the respondent organisation has adequately dealt with the complaint. Complaints are closed using this provision in the Act where the respondent was found to be in breach of the Act and then took adequate steps to resolve the matter and where the respondent adequately resolved the matter without a formal investigation having been commenced. As such, an analysis of the number of complaints closed as adequately dealt with provides an indication of the number of complaints that were substantiated.
The following graph shows the breakdown of issues in complaints closed on the grounds that the respondent had adequately dealt with the privacy issues raised.

![Privacy Complaints Resolved by the Respondent following Intervention by the OPC](image)

Complaints closed from 21 Dec 01 - 31 Jan 05

It is noteworthy, that whilst disclosure was the most commonly raised issue in complaints received by the Office, a much smaller proportion of complaints closed as adequately dealt with, concerned disclosure issues. Conversely, the figures suggest that a disproportionate number of complaints concerning access issues were substantiated, requiring action on the part of the respondent to resolve the matters raised.
Complaints by Respondent Sector

The following graph shows the number of NPP complaints received according to industry sector, with finance sector organisations most frequently named as respondents in the NPP complaints received, followed by health and telecommunications sector organisations.

Again, these figures can be compared with the number of NPP complaints closed where the respondent took action to resolve the privacy issue. In this case, the number of complaints closed as adequately dealt with was, generally speaking, proportional to the number of complaints received against that sector.
Enquiries Statistics

The OPC has received 67,486 phone enquiries and 6353 written enquiries since the introduction of the private sector provisions in the Privacy Act (21 December 2001 – 31 January 2005).

Of the phone enquiries received 43484 (64%) specifically concerned the private sector provisions in the Act (the NPPs). Similarly, 65% (4124) of written enquiries concerned the NPPs.

More than half of the NPP enquiries received by the Office were made by individuals seeking advice regarding their privacy rights. Specifically, 65% of phone enquiries and 56% of written enquiries concerning the NPPs were made by individuals. The remaining enquiries were largely received from organisations seeking advice about their responsibilities under the Act, or advice regarding the application of the Act in general.

The number of phone and written enquiries received increased significantly following the introduction of the private sector provisions in the Act in December 2001, and has since remained fairly stable, as shown in the following graphs:

### Phone Enquiries Received by Financial Year

<table>
<thead>
<tr>
<th>Year</th>
<th>Enquiries</th>
</tr>
</thead>
<tbody>
<tr>
<td>2000-2001</td>
<td>8177</td>
</tr>
<tr>
<td>2001-2002</td>
<td>21033</td>
</tr>
<tr>
<td>2002-2003</td>
<td>21290</td>
</tr>
<tr>
<td>2003-2004</td>
<td>20207</td>
</tr>
</tbody>
</table>

### Written Enquiries Received by Financial Year

<table>
<thead>
<tr>
<th>Year</th>
<th>Enquiries</th>
</tr>
</thead>
<tbody>
<tr>
<td>2000-2001</td>
<td>884</td>
</tr>
<tr>
<td>2001-2002</td>
<td>2700</td>
</tr>
<tr>
<td>2002-2003</td>
<td>2382</td>
</tr>
<tr>
<td>2003-2004</td>
<td>2206</td>
</tr>
</tbody>
</table>
Enquiries by Issue Type

As with complaints received by the Office, the issues raised in enquiries tend to cluster around a few of the privacy principles, in particular, the principles dealing with use and disclosure (NPP 2), collection (NPPs 1 & 10) and access (NPP 6). A significant number of enquiries received also concerned the exemptions to the NPPs, such as the employee records exemption and the small business operator exemption.

The following graphs show the numbers of NPP phone and written enquiries received respectively according to issue type.
Enquiries by Industry Sector

The following graphs show the numbers of NPP phone and written enquiries received according to industry sector. For both phone and written enquiries, the industry sector about which the most enquiries were received was the health sector.
Appendix 10

Own Motion (section 40 (2)) power

Current Criteria for conducting own motion investigations

A decision to launch an own motion investigation is a matter of judgment. Factors that the Commissioner takes into account in making this decision include:

- sensitivity of the personal information involved
- number of people affected and the consequences for those individuals
- likelihood that the investigation will reveal acts or practices that involve systemic interferences with privacy and/or that are widespread
- expertise and resources available to the Office
- progress of an agency or organisation’s own investigation into the matter
- nature of any proposed resolution
- necessity for the Office to be satisfied that the investigation is complete and/or proposed resolutions are implemented and
- general public and parliamentary expectations that if it becomes aware of a breach, the Office will investigate where appropriate.

Own motion investigations 2003-04

Situations the Commissioner investigated or made inquiries into during 2003/2004 include:

- 6000 medical records abandoned in a building – the records are now in the safe custody of the medical practitioner concerned
- web sites that could be manipulated easily to get access to third party details – website security has been enhanced
- a telephone system that recorded digits including pin numbers – software changes have removed this risk
- improper access to records held by a credit reporting agency – generally no breach found but some system changes to ensure accesses properly recorded.
Own motion investigations December 2001 - February 2005

Own Motion Investigations recorded by sector code from December 2001 to February 2005 are as follows:

<table>
<thead>
<tr>
<th>Sector</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Federal Government</td>
<td>18.0</td>
</tr>
<tr>
<td>Finance/Investment/Share Registers/and Pawnbrokers</td>
<td>15.5</td>
</tr>
<tr>
<td>Health Service Providers (including pharmacists)</td>
<td>12.5</td>
</tr>
<tr>
<td>Telecommunications/ISPs</td>
<td>8.5</td>
</tr>
<tr>
<td>Private Investigator/Debt Collector/Credit Reference Agencies/Tenancy Databases</td>
<td>8.5</td>
</tr>
<tr>
<td>Legal, Accounting and Management Services</td>
<td>4.5</td>
</tr>
<tr>
<td>Insurance</td>
<td>4.5</td>
</tr>
<tr>
<td>Personal and Other Services – General</td>
<td>3.5</td>
</tr>
<tr>
<td>Retail</td>
<td>3.0</td>
</tr>
<tr>
<td>Market Research and Direct Marketing</td>
<td>2.5</td>
</tr>
<tr>
<td>Landlords/Real Estate Agents/Developers</td>
<td>2.5</td>
</tr>
<tr>
<td>IT/Architects/Surveyors/Engineers</td>
<td>2.5</td>
</tr>
<tr>
<td>Theatres/Libraries/Sport/Media</td>
<td>1.5</td>
</tr>
<tr>
<td>ACT Government</td>
<td>1.5</td>
</tr>
<tr>
<td>Property and Business Services – General</td>
<td>1.5</td>
</tr>
<tr>
<td>Postal and Courier Services</td>
<td>1.5</td>
</tr>
<tr>
<td>Electricity, Gas and Water Supply</td>
<td>1.5</td>
</tr>
<tr>
<td>Other</td>
<td>1.0</td>
</tr>
<tr>
<td>Business and Professional Associations</td>
<td>1.0</td>
</tr>
<tr>
<td>Airlines/Travel Agents/Removalists/Storage</td>
<td>1.0</td>
</tr>
<tr>
<td>Superannuation</td>
<td>0.5</td>
</tr>
<tr>
<td>Political/Lobby and Clubs/Interest Groups</td>
<td>0.5</td>
</tr>
<tr>
<td>Manufacturing</td>
<td>0.5</td>
</tr>
<tr>
<td>Hire Household Goods/Equipment</td>
<td>0.5</td>
</tr>
<tr>
<td>Education</td>
<td>0.5</td>
</tr>
<tr>
<td>Charities</td>
<td>0.5</td>
</tr>
<tr>
<td>Employment Services</td>
<td>0.5</td>
</tr>
</tbody>
</table>
Appendix 11

Current Powers to enforce determinations

The Privacy Act allows the Office to take certain action to assess compliance with a determination, for instance the Office may:

- request information from the respondent to assess their compliance with the Determinations
- collect information from other sources (for example from persons who were complainants in the original complaint against the respondent) that is relevant to an assessment of whether or not the respondent is complying with the Determinations
- visit the respondent’s premises and examine their systems with their consent
- compel the production of documents under section 44 in the event of another investigation being conducted into the respondent’s operations under Division 1 of Part V of the Privacy Act
- authorise a person to enter the respondent’s premises and inspect their documents pursuant to section 68 – that person can then seek a warrant from a Magistrate to allow entry into the respondent’s premises if the Magistrate is satisfied that it is ‘reasonably necessary’
- commence proceedings for enforcement of the Determinations and seek an interim injunction or orders for discovery.
Appendix 12

Decision Appeal Processes in comparable legislation

Human Rights and Equal Opportunity Commission

Under section 46PO of the Human Rights and Equal Opportunity Commission Act 1986, if a complaint has been terminated by the president under section 46PE or 46PH and the President has given a notice under subsection 46PH(2) in relation to the termination, any person affected in relation to the complaint may make an application to the Federal Court or the Federal Magistrates Court, alleging unlawful discrimination by one or more of the respondents to the terminated complaint. A complaint may be terminated for example if the President is satisfied that the alleged unlawful discrimination is not unlawful discrimination (section 46PH(1)(a)) or if the President is satisfied that there is no reasonable prospect of the matter being settled by conciliation (section 46PH(1)(i)). Powers to conciliate matters under the Human Rights and Equal Opportunity Commission Act do not extend to the making of determinations.

PRIVACY NSW

As well as making a complaint to the Privacy Commissioner under section 45 of the Act, an aggrieved individual may request an internal review under section 53. Under section 55 of the Privacy and Personal Information Protection Act 1998 (NSW), if a person who has made an application for internal review is not satisfied with the findings of the review or the action taken by the public sector agency in relation to the application, the person may apply to the Administrative Decision Tribunal for a review of the conduct that was the subject of the application.

Under Subsection 47(1) of the Health Records Information Privacy Act 2002, the NSW Privacy Commissioner may make a written report as to any findings or recommendations by the Privacy Commissioner in relation to a complaint dealt with by the Privacy Commissioner. Under section 48, if a complaint is the subject of a report by the Privacy Commissioner, a person who has made a complaint to the Privacy Commissioner may apply to the Tribunal for an inquiry into the complaint.

PRIVACY VICTORIA

Under section 37 of the Information Privacy Act 2000 (Vic) and section 63 of the Health Records Act 2001 (Vic), if conciliation by the Privacy or Health

259 Established by the Administrative Decisions Tribunal Act 1997.
Services Commissioner is unsuccessful, the complainant may refer the matter to the Victorian Civil and Administrative Tribunal\textsuperscript{260}.

**PRIVACY New Zealand**

Under section 83 of the Privacy Act 1993 (NZ), an aggrieved individual may bring proceedings before the Complaints Review Tribunal if the Commissioner believes that the complaint does not have substance or that the matter ought not to be proceeded with or where the Proceedings Commissioner agrees to the individual bringing proceedings or declines to take proceedings.

**ANTI-DISCRIMINATION NSW**

Under section 91 of the Anti-Discrimination Act 1977 (NSW), a complainant may require the President to refer the complaint to the Administrative Decisions Tribunal where the President has given a notification. The President may give a notification if the President is satisfied that the complaint is frivolous, vexatious, misconceived or lacking in substance, or that for any other reason the complaint should not be entertained (section 90(1)).

**ANTI-DISCRIMINATION QLD**

If the Commissioner believes a complaint under the Anti-Discrimination Act 1991 (Qld) cannot be resolved by conciliation, the complainant may require the Commissioner to refer the complaint to the tribunal under section 164A or 166.

**ANTI-DISCRIMINATION TAS**

Under section 65 of the Anti-Discrimination Act 1998 (Tas), a complainant may have a rejected complaint reviewed by the tribunal. The Commissioner may reject a complaint for example if in the opinion of the Commissioner, it is trivial, vexatious, misconceived or lacking in substance (section 64(1)(a) or the subject matter of the complaint has already been adequately dealt with by the Commissioner, a State authority or a Commonwealth statutory authority (section 64(1)(f)).

\textsuperscript{260} Established by the Victorian Civil and Administrative Tribunal Act 1998.
Appendix 13

Demographic information about complainants

As noted in the issues paper the Office had not previously collected demographic information about complainants. To assist the Office identify which sections of the community were making privacy complaints to the Office, it undertook a three month complainant demographic survey in December 2004, January 2005 and February 2005.

The Office wrote to all complainants who submitted a complaint during this time (not just complaints relating to the NPPs) and asked that they complete the survey and return it in a reply paid envelope. Complainants were advised that completing the survey was voluntary and that if they did not complete the survey it would not affect the way in which the Office dealt with their complaint. Complainants were also advised that the survey was anonymous and that the information collected was de-identified.

The Office sent the survey to approximately 250 individuals and received only 36 surveys in reply. This number of responses is too small to rely on as an accurate representation of total complainants. However, the Office was able to extract information from its complaint management software that suggests, at least in respect of gender, the survey results may be representational.

The results of the survey are described below. However the Office stresses that it is not known if the results accurately reflect its client group. The Office has decided to continue with the complainant demographic survey and it has become part of the standard complaint acknowledgement process.

Complainant Demographic Results

67% of complainants were male and 33% were female.

More complainants were between the ages of 40-49.
None of the complainants were Aboriginal or Torres Strait Islanders.

The majority of complainants (68%) were born in Australia and 20% were born in the UK. Other countries of birth stated by respondents were Canada, Fiji, Singapore and Sri Lanka.

Nearly all complainants (92%) listed English as the main language spoken in their home. Other respondents listed English and at least one other language spoken in their home and a few surveys noted another language as the main language in their home.

More complainants (71%) live in a capital city than anywhere else or a major regional centre (17%).

The level of education completed by complainants was varied. Over half of the complainants had completed a Diploma/Advanced Diploma, Bachelor degree or Post-graduate degree.

Respondents listed the income category $0 - $25 000 more often than other categories. However, 65% of respondents earned over $25 000 with 15% earning over $75 000.

The majority of complainants (83%) do have access to the internet.

Complainants found out about the Office through many different avenues including lawyers, community organisations, government agencies, friends or family and the Internet or a website.
Appendix 14

Complainant and respondent satisfaction survey

Background and methodology

The survey was conducted in February and March 2005. The purpose of the survey was to gauge the opinion of complainants and respondents with respect to the Office’s complaint handling process and to seek suggestions from complainants and respondents about any possible improvements to the complaint handling service. The complainants and respondents interviewed were involved in the Office’s complaint handling process but were not necessarily involved in complaints relating to the NPPs.

In all, the Office interviewed 41 organisations and 100 individuals. All those surveyed were given a notice in accordance with IPP 2 and NPP 2.

There are a number of concerns about the ability to rely on the representative nature of the completed surveys. This is because the method of selecting the subjects for the survey relied heavily on the use of the telephone and favoured those complainants and respondents who were more readily available by phone in the given time period (March 2005).

Out of the 100 matters that were the subject of the interview 68 were Investigations under section 40(1), 21 preliminary inquiries under section 42 and in 11 cases the Office had declined to investigate the matter under section 40(1) or (2).

Results

1 Timeliness

- 58% of complainants thought that the complaints were not handled in a timely manner.
- 22% of respondents thought that the complaint was not handled in a timely manner. 63% thought that the handling was timely.
2 Impartiality

- 44% of complainants thought that the staff acted fairly towards the parties
- 89% of respondents thought that the staff acted fairly towards the parties

3 Access to information about the complain handling process

- 72% of complainants thought that the explanations given by the office were clear and 77% understood the forms and correspondence
- 93% respondents thought that the explanations given by the office were clear and 93% understood the forms and correspondence and found them clear.

4 How well reasons for the decisions are communicated

- 63% of complainants thought that they were given clear reasons for the decisions.
- 78% of respondents thought that they were given clear reasons for the decisions.
5 Method of communication

It appears that both complainants (44%) and respondents (66%) prefer hard copy correspondence.

6 Level of satisfaction

Service

There were mixed messages about the overall level of satisfaction with the service by the complainants

- 41% of complainants rated it as poor but
- 39% as either good or excellent.

Respondents generally were more satisfied with the service, 56% rating it as either good or excellent.

The difference in the responses provided by the Complainant and the Respondent and their levels of satisfaction are illustrated by the following table:

<table>
<thead>
<tr>
<th>LEVEL OF SERVICE RECEIVED</th>
<th>Complainants</th>
<th>Respondents</th>
</tr>
</thead>
<tbody>
<tr>
<td>excellent</td>
<td>12%</td>
<td>14%</td>
</tr>
<tr>
<td>very good</td>
<td>13%</td>
<td>17%</td>
</tr>
<tr>
<td>good</td>
<td>13%</td>
<td>13%</td>
</tr>
<tr>
<td>satisfactory</td>
<td>20%</td>
<td>25%</td>
</tr>
<tr>
<td>poor</td>
<td>41%</td>
<td>3%</td>
</tr>
</tbody>
</table>

Outcomes

86% of respondents and 43% of complainants were satisfied with the outcomes of the complaints. 56% of complainants were dissatisfied.
7 Other Suggestions

Most of the suggestions focused on the need to “speed up the process” and to make it more transparent. Some focused on the need to remove the exceptions, particularly small business, and to give the Office more power and resources to investigate the complaints.

A number of the respondents commented favourably on the queue referral system and welcomed additional opportunities to resolve the matter directly with customers.