CHAPTER 4

PRIVATE SECTOR PROVISIONS

4.1 This chapter will consider issues raised in submissions and evidence in relation to the effectiveness of the Privacy Act in the private sector, including:

- the review of the private sector provisions[1] by the Privacy Commissioner;
- the general reaction to private sector provisions, including consistency issues;
- exemptions from the private sector provisions; and
- other issues in relation to the private sector provisions.

4.2 It is noted that some concerns raised in submissions and discussed below may apply not only to the private sector, but could also impact on the public sector.

Review of the private sector provisions by the Privacy Commissioner

4.3 In August 2004, the Attorney-General asked the Privacy Commissioner to review the operation of the private sector provisions of the Privacy Act 1998 (OPC review). The OPC review's terms of reference overlapped with the terms of reference of this inquiry. However, the terms of reference for the OPC review excluded consideration of: genetic information; employee records; children's privacy; electoral roll information and the related exemption for political acts and practices. The justification for exclusion from that inquiry was that these areas are currently, or have recently been, the subject of separate review.[2] The credit reporting provisions in Part IIIA of the Privacy Act were also not reviewed, although those provisions were considered where relevant to the operation of the private sector provisions.[3]

4.4 Indeed, the APF described the terms of reference for the OPC review as 'unnecessarily restrictive' and believed that they resulted 'in a review report which attempts to draw conclusions in somewhat of a vacuum.'[4] Further, the APF felt that:

> Key issues in current privacy debates, such as employee privacy, and the role of mass surveillance and dataveillance, are ignored. [5]

---

1 Note: references to the 'private sector provisions' of the Privacy Act refer to those provisions contained in the *Privacy Amendment (Private Sector) Act 2000.*

2 OPC review, Appendix 1.

3 OPC review, pp 22-23.

4 *Submission 32B*, p. 1.

5 *Submission 32B*, p. 7.

4.5 An issues paper relating to the OPC review was released in October 2004,[6] and that inquiry received 136 submissions.[7] The OPC also held consultation meetings in each capital city in November and December 2004.[8]

4.6 The Privacy Commissioner was asked to report to the Attorney-General by 31 March 2005. The OPC review was released publicly on 18 May 2005. The review also concluded that, on balance, the private sector provisions of the Privacy Act have 'worked well'.[9] Nevertheless, the review made 85 recommendations about how the operation of the private sector provisions could be improved.[10] As the Privacy Commissioner, Ms Karen Curtis, explained to the committee:

> The essential finding is that on balance the provisions of the private sector amendment act have worked well. I have to say that business thinks they have worked better than consumers think but there was no significant evidence that there was any fundamental flaw with the provisions. However, I have still made 85 recommendations which go to finetuning a number of the provisions, making some higher level suggestions and recognising that there are many actions and activities that my office can undertake to improve the way the provisions are understood by the community and by business.[11]

4.7 Some of the Privacy Commissioner's key recommendations are considered where relevant in this chapter. However, it is worth noting at the outset that the review made an overarching recommendation that:

> 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.[12]

4.8 In response to the committee's questions as to what kind of review might best serve this purpose, the OPC responded that:

> …any future review process would require appropriate resources, an adequate time frame, extensive consultation, an international perspective and the ability to draw upon a wide range of technical expertise to ensure comprehensive and workable recommendations.[13]

---

6 Available at: http://www.privacy.gov.au/act/review/ispap2004.pdf (accessed 23 March 2005).

7 Available at: http://www.privacy.gov.au/act/review/reviewsub.html (accessed 23 May 2005).

8 OPC review, p. 25; see also Ms Karen Curtis, OPC, *Committee Hansard*, 19 May 2005, p. 47.

9 Ms Karen Curtis, OPC, *Committee Hansard*, 19 May 2005, p. 47; see also OPC review, p. 2.

10 OPC review, p. 8.

11 *Committee Hansard*, 19 May 2005, p. 47.

12 OPC review, p. 8.

13 *Submission 48*, p. 6.

4.9 The OPC further suggested that the review could be a joint project between the ALRC and the OPC or the Attorney-General's Department.[14]

4.10 The committee notes the Special Minister of State, Senator the Hon. Eric Abetz, recently supported this recommendation.[15] This recommendation was also supported by the APF, although the APF disagreed with the OPC's conclusion that the 'provisions work well on balance', arguing that this conclusion 'is not supported by the statements later in the report's discussion.'[16] Further, the APF expressed its disappointment that:

> …the review report fails to assess whether or not privacy protection has improved in a meaningful way since the introduction of the private sector provisions. The focus instead appears to mostly be on how well business has coped with the change. In general therefore, the tone of the analysis and the recommendations appear to give more weight to the concerns of business than either the individual or the public interest.[17]

General reaction to private sector provisions

4.11 During this inquiry, several submissions were generally supportive of the current legislative regime for the private sector.[18] The bank, ANZ, for example, felt that the NPPs and other private sector provisions are 'generally working well', and that 'further legislative amendment is not required at this stage.'[19] Similarly, the Fundraising Institute of Australia (FIA), expressed the view that further restriction on the use of personal information is 'not appropriate, as there is a lack of sufficient evidence that the Privacy Act, including the National Privacy Principles (NPPs), is not meeting its objectives'.[20]

4.12 Some submissions also expressed support for the 'high level', flexible approach taken in the private sector provisions and the NPPs.[21] In contrast, other

---

14 *Submission 48*, p. 6.

15 Senator Abetz is the Federal Minister responsible for the Australian Government Information Management Office and the Commonwealth's whole-of-government *e-government* agenda. Senator The Hon. Eric Abetz, Special Minister of State, *Privacy Key in E-Government*, media release A0523, 6 June 2005; see also James Riley, "Abetz calls for privacy review", *The Australian,* 7 June 2005, p. 30.

16 *Submission 32B*, p. 2.

17 *Submission 32B*, p. 2.

18 See, for example, ANZ, *Submission 6*, pp 2-3; FIA, *Submission 3*, p. 4; Baycorp Advantage, *Submission 43*, p. 3.

19 *Submission 6*, pp 2-3, 6.

20 *Submission 3*, p. 4.

21 See, for example, FIA, *Submission 3*, p. 7; Australian Chamber of Commerce and Industry (ACCI), *Submission 25*, p. 2.

argued that the provisions and NPPs are 'too high level'.[22] For example, Ms Irene Graham of EFA argued that:

> …you can interpret certain aspects of the national privacy principles to the left or to the right, so to speak. They can be interpreted to have a privacy protective intent or you can interpret various words and phrases slightly differently and produce a non-privacy-protective intent that favours the business as distinct from individual whose privacy is concerned.[23]

4.13 Ms Graham explained that the national privacy principles were only ever intended to be high level principles because it was anticipated that industries would develop more detailed rules and regulations within an industry code.[24] However, Ms Graham then observed that:

> Virtually no industry codes have been developed at all…Therefore, we have all been left with high level principles that often you can argue till kingdom come as to what this particular privacy principle means in relation to this specific disclosure of information.[25]

4.14 Some submissions felt that there were other significant problems with the private sector provisions, and suggested significant changes to the private sector provisions including the NPPs.[26] For example, the APF argued that:

> The private sector provisions do not in our view strike an appropriate balance with competing interests in that the provisions themselves (and the exemptions) excessively favour public interests (primarily those supporting commercial interests) that intrude on privacy.[27]

4.15 Similarly, EFA expressed the view that:

> Instead of empowering individuals to exercise their right to privacy of personal data, the private sector provisions have conferred on business interests the right to invade individual privacy.[28]

4.16 In contrast, Mr Andrew Want of Baycorp Advantage acknowledged that there may be a need for some regulatory reform, but expressed Baycorp's view that the Privacy Act:

---

22 See, for example, Ms Irene Graham, EFA, *Committee Hansard*, 22 April 2005, p. 47.

23 *Committee Hansard*, 22 April 2005, p. 47.

24 *Committee Hansard*, 22 April 2005, p. 47.

25 *Committee Hansard*, 22 April 2005, p. 47. Note that industry privacy codes are considered further later in this chapter.

26 APF, *Submission 32*, pp 15-18; EFA, *Submission 17*, pp 38-45; see also Mr Roger Clarke, *Submission 28*, p. 4 and Addendum.

27 *Submission 32*, p. 12.

28 *Submission 17*, p. 7.

> ...has proved to be a very strong framework for privacy regulation and has stood Australia very well over the last several years.[29]

Consistency

Inconsistency with other Commonwealth, State and Territory legislation

4.17 A key concern raised during the committee's inquiry was the considerable level of inconsistency between the Privacy Act and other Commonwealth, state and territory legislation.[30]

4.18 Yet one of the stated objectives of the private sector provisions introduced by the Privacy Amendment (Private Sector) Bill 2000 to achieve consistency. The former Attorney-General stated during the second reading speech to the Privacy Amendment (Private Sector) Bill 2000 that:

> The Privacy Amendment (Private Sector) Bill 2000 provides a national, consistent and clear set of standards to encourage and support good privacy practices. safeguards are in place.[31]

4.19 He further explained that:

> By introducing this bill, the Commonwealth intends to establish a single comprehensive national scheme for the protection of personal information by the private sector. However, state and territory laws will continue to operate to the extent that they are not directly inconsistent with the terms of the bill. [32]

4.20 However, when submitters and witnesses referred to privacy regulation in Australia, the words 'patchwork' and 'fragmented' arose frequently during the committee's inquiry. For example, the ACA observed that:

> We are concerned that what is emerging is a patchwork of privacy protection, driven in various ways by divisions between public and private sectors of the economy, state and federal levels of government, specific economic sectors (such as health), emerging technologies all of which have subverted the aim of the legislation in this regard. Not least of the drivers for these divisions are the gaps embodied in the federal legislation (such as

---

29 *Committee Hansard*, 19 May 2005, p. 1.

30 See, for example, Real Estate Institute of Australia, *Submission 1*, p. 2; FIA, *Submission 3*, p. 4; ANZ, *Submission 6*, pp 4-5; AMA, *Submission 9*, p. 3; Queensland Institute of Medical Research (QIMR), *Submission 13*, p. 7; ACA, *Submission 15*, p. 14; Caroline Chisholm Centre for Health Ethics, *Submission 21*, p. 11; ACCI, *Submission 25*, p. 2; APF, *Submission 32*, p. 5; ADMA, *Submission* 38, p. 4.

31 The Hon Daryl Williams AM QC MP, former Attorney-General, *House of Representatives Hansard*, 12 April 2000, p. 15749.

32 The Hon Daryl Williams AM QC MP, former Attorney-General, *House of Representatives Hansard*, 12 April 2000, p. 15751; see also OPC review, p. 32.

> the small business exemption and employee record exception) that was intended to deliver the nationally consistent scheme.[33]

4.21 Similarly, the APF expressed their view that:

> There is a major and growing problem of inconsistency between federal and State and Territory privacy laws. This stems largely from the failure of the Commonwealth to ensure that the federal law provided adequate protection across the board. Had it done so, a major objective of the 2000 amendments – to provide a consistent national framework, might have been realized. But it is hardly surprising that, faced with major gaps and weaknesses, the States and Territories have felt it necessary to provide their citizens with additional protection both in general privacy laws and in specific areas of health privacy and surveillance.[34]

4.22 The OPC review made a number of recommendations to address the issue of inconsistency.[35] As the Privacy Commissioner, Ms Karen Curtis, explained to the committee:

> The biggest issue is national consistency. It has not been achieved throughout the first three years of the operation of the act. It is probably for a variety of reasons: the environment has changed in some ways; security concerns; and the fact that exemptions under the act, for instance, may have led some states and territories to develop their own laws. I am specifically referring to workplace surveillance in New South Wales, and it is also mooted in Victoria. That is a key issue for us, especially in the areas of health and telecommunications.[36]

4.23 In particular, the OPC recommended that 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.[37] The review report explained:

> 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.[38]

4.24 The OPC review further stated that '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

---

33 *Submission 15*, p. 15.

34 *Submission 32*, p. 5.

35 OPC review, Recommendations 2-16, pp 8-9.

36 *Committee Hansard*, 19 May 2005, p. 48.

37 OPC review, Recommendation 2, pp 45, 48.

38 OPC review, p. 45.

barrier to doing so.'[39] The review therefore suggested that 'section 3 could be amended to make it clear that the Privacy Act was intended to cover the field.'[40]

4.25 However, the APF expressed considerable caution about this recommendation, arguing that the 'significant gaps' in the coverage of the Privacy Act should be addressed first, such as the exemptions for employee records, small business, the media and political parties. The APF argued that:

> If those gaps were first filled, the States and Territories would have less demand to legislate for their own jurisdictions.[41]

4.26 Indeed, the OPC itself conceded that 'the exemptions in the Privacy Act are undermining the goal of national consistency.'[42] Some of these exemptions are considered later in this chapter.

Inconsistency with other specific legislation

4.27 Many submissions raised specific examples of inconsistency between the Privacy Act and other legislation. As noted in the previous chapter, several submitters were concerned about inconsistency between the Privacy Act and surveillance and telecommunications legislation.[43] Indeed, the submission from EFA contained a detailed comparison and analysis of inconsistencies between the Privacy Act and the *Telecommunications Act 1997* (Telecommunications Act).[44] Ms Irene Graham from EFA explained to the committee:

> We feel that the way the Privacy Act was introduced in 2000 did not look closely enough, probably completely unintentionally, at where there were variances between those two laws. We feel that there needs now to be some amendments made to the Telecommunications Act to make it consistent with the Privacy Act or, alternatively, amendments made to the Privacy Act to make it clear that the Telecommunications Act does not override the Privacy Act. There is just an imbalance there with some of the provisions.[45]

4.28 The issue of inconsistency in relation to telecommunications was also considered by the OPC review of the private sector provisions.[46] In particular, the report recommended that:

---

39 OPC review, p. 45.

40 OPC review, p. 45; and see also Ms Karen Curtis, OPC, *Committee Hansard*, 19 May 2005, p. 48.

41 *Submission 32B*, p. 4.

42 OPC review, p. 45.

43 See, for example, APF, *Submission 32*, p. 9; EFA, *Submission 17*, pp 7-17 and Appendix 1.

44 *Submission 17*, Appendix 1, pp 48-54.

45 *Committee Hansard*, 22 April 2005, p. 42.

46 OPC review, pp 49-62.

> 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.[47]

4.29 The OPC also proposed that it would discuss certain matters 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; and also between the private sector provisions of the Privacy Act and the *Spam Act 2003*.[48]

4.30 Many submissions raised the health sector as an area where inconsistency of Commonwealth, state and territory legislation was particularly problematic.[49] This issue is considered separately in more detail in chapter 5.

4.31 Other examples of inconsistent legislation were also raised. For example, at the State level, ANZ noted that several states were considering introducing legislation relating to workplace surveillance, which could result in non-uniform laws throughout Australia. ANZ felt this would be particularly problematic for businesses operating at a national level.[50] This issue is also considered later in this chapter in the discussion on the employee records exemption.

4.32 The Real Estate Institute of Australia raised the range of legislation relating to residential tenancy databases, which it argued is 'impacting negatively on consumers and business.'[51] The Institute supported a nationally consistent framework for the operation of tenancy databases.[52] Indeed, the OPC review specifically addressed the issue of tenancy databases.[53] The report notes that:

> 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-

---

47 OPC review, Recommendation 8, p. 63; see also APF, *Submission 32B*, p. 4.

48 OPC review, Recommendations 10-11, p. 63.

49 See, for example, APF, *Submission* 32, pp 8-9; Centre for Law and Genetics, *Submission* 24, pp 4-5; NHMRC, *Submission 20*, pp 7-8 and Attachment D; see also Anna Johnston, APF, *Committee Hansard*, 19 May 2005, p. 19; Mr Charles Britton, ACA, *Committee Hansard*, 19 May 2005, p. 26; Professor Don Chalmers, Centre for Law and Genetics, *Committee Hansard*, 20 May 2005, p. 9; Ms Pamela Burton, AMA, *Committee Hansard*, 20 May 2005, p. 15.

50 *Submission 6*, p. 5; see also ACA, *Submission 15*, p. 4.

51 *Submission 1*, p. 2; see also OPC, *Media Release: Tenancy database operator breaches the Privacy Act*, 19 April 2004.

52 *Submission 1*, p. 2; see also OPC, *Media Release: Tenancy database operator breaches the Privacy Act*, 19 April 2004.

53 OPC review, Recommendations 14-16, pp 72-73.

> General's Department of the Australian Government. The working party intends to report to MCCA and SCAG by the middle of 2005.[54]

4.33 The OPC review recommended that the work being undertaken by this working party should be advanced as a high priority.[55] Depending on the outcome of this work, the OPC review also recommended that the Australian Government consider making the Privacy Act apply to all residential tenancy databases. The OPC review explained that:

> 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.[56]

4.34 The OPC review also noted that, if the Privacy Act is amended to provide for a power to make a binding code (under recommendation 7), the Privacy Commissioner could make a binding code that applies to tenancy databases.[57]

Consistency between public and private sector

4.35 Several submissions were also concerned about the inconsistency within the Privacy Act itself as a result of the differing regimes applying to the private and public sectors. Some submissions suggested the regulation of government agencies and private sector organisations should be harmonised.[58] In particular, it was suggested that the NPPs and the IPPs should be merged, with one set of principles applying to all sectors.[59] For example, the APF argued that:

> The distinction between the public and private sectors is increasingly artificial and there is no good reason to maintain two separate sets of principles. Government services are increasingly being delivered by the private sector, whether under contract or by other arrangements. It is confusing to individuals and organisations to have different principles trying to achieve the same underlying objectives. The IPPs and NPPs should be merged…[60]

4.36 Similarly, the Victorian Privacy Commissioner, Mr Paul Chadwick supported harmonisation of the NPPs and IPPs, commenting that:

---

54 OPC review, p. 73.

55 OPC review, Recommendation 14, p. 73.

56 OPC review, Recommendation 15, p. 73; see also Recommendation 53.

57 OPC review, Recommendation 16, p. 73.

58 See, for example, EFA, *Submission 17*, p. 37; APF, *Submission 32*, p. 6; Victorian Privacy Commissioner, *Submission 33*, p. 4.

59 APF, *Submission 32*, p. 6.

60 *Submission 32*, p. 6.

> One reason why that is so significant is that, of course, since 1980, a dramatic change has happened in what used to be the sharp barrier between the public and private sectors. Many public functions are now provided by the private sector through outsourcing and, in the most dramatic examples, privatisation. That means that the public is sometimes reacting to a request for personal information made by government under law for a public task, but the practicalities of protecting that data and keeping it accurate et cetera are happening in the back office of a contracted service provider, sometimes offshore. So it just makes sense to have one set of principles with enough flexibility for the relevant decision makers to apply them intelligently in the many different settings in which you find them.[61]

4.37 As outlined above, the two separate regimes can be especially problematic in the health sector where public and private health organisations often work closely together. It is also problematic where private sector contractors are engaged by government agencies.[62] The committee also notes that other jurisdictions, such as New Zealand, have one set of privacy principles applying across all sectors.[63]

4.38 The OPC discussed and acknowledged this issue in its review:

> 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.[64]

4.39 The OPC review observed that:

> 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.[65]

4.40 Finally, the OPC review recommended that:

---

61 *Committee Hansard*, 22 April 2005, p. 6.

62 See, for example, EFA, *Submission 17*, p. 37; APF, *Submission 32*, p. 6; Department of Health and Ageing, *Submission 34*, pp 21-22.

63 Office of the Privacy Commissioner, New Zealand, Fact Sheet No. 1, *A Guide to the Privacy Act 1993,* at: http://www.privacy.org.nz/people/peotop.html (accessed 9 June 2005).

64 OPC review, p. 46.

65 OPC review, p. 46.

> 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.[66]

Exemptions in the Privacy Act

4.41 As outlined in chapter 2 of this report, the Privacy Act contains a number of exemptions and exceptions, many of which drew considerable criticism during the committee's inquiry. And as mentioned above, some submitters felt that one of the key factors contributing to inconsistency is the exemptions in the Privacy Act. Some of the key exemptions will be discussed in turn below, and include:

- small business exemption;
- media exemption;
- employee records exemption;
- political acts and practices exemption; and
- direct marketing exceptions.

Small business exemption

4.42 The small business exemption in the Privacy Act drew a considerable amount of comment in submissions. As outlined in chapter 2, small businesses with an annual turnover of $3 million or less are generally exempted from the operation of the Privacy Act.[67] Small businesses may also voluntarily opt-in to comply with the Privacy Act. The OPC review indicates that 130 small businesses have opted in to coverage by the Privacy Act.[68]

4.43 The OPC review of the private sector provisions indicated that 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. Secondly, it is necessary to balance privacy protection against the need to avoid unnecessary cost on small business.[69]

---

66 OPC review, Recommendation 5, p. 48.

67 Privacy Act, section 6D. However, note that there some exceptions: see subsections 6D(4)-(9).

68 OPC review, p. 179.

69 OPC review, p. 179.

4.44 During this inquiry, several submissions supported the small business exemption under the Privacy Act.[70] For example, the Real Estate Institute of Australia, noting that the majority of real estate business are small businesses, argued that:

> …regulating the information flow between clients and small businesses through the Privacy Act is not the best way to achieve good business practices or consumer protection. Such increased regulation would only add to the cost burdens faced by small businesses, making them less competitive or even unviable. The end result of such increased regulation would be industry sectors dominated by large businesses.[71]

4.45 Others were critical of the small business exemption.[72] It is noted that the exemption is probably the key outstanding issue preventing recognition of the adequacy of Australia's privacy laws under the European Union's Data Protection Directive (this is discussed further later in this chapter). The committee also notes that the New Zealand *Privacy Act 1993* does not have a similar small business exemption, but rather the New Zealand legislation covers all businesses whether large or small, government or non-government.[73]

4.46 Some submissions suggested that the small business exemption should be removed altogether.[74] For example, EFA argued that:

> Privacy rights do not disappear just because a consumer happens to be dealing with a small company. The responsibility upon commercial organisations to recognise the privacy rights of consumers does not magically become apparent when an organisation's revenue base exceeds some arbitrary figure. Individuals are rarely able to know whether or not an organisation is a small business for the purposes of the PA [Privacy Act] since annual turnover figures are rarely publicly disclosed.[75]

4.47 In the same vein, the APF described the small business exemption as 'too broad, but also too complex', and argued that:

---

70 See, for example, Real Estate Institute of Australia, *Submission 1*, p. 3; ACCI, *Submission 25*, pp 4-7.

71 *Submission 1*, p. 3.

72 See, for example, Caroline Chisholm Centre for Health Ethics, *Submission 21*, p. 12; Dr Anthony Place, *Submission 22*, p. 4; EFA, *Submission 17*, pp 34-35; APF, *Submission 32*, p. 14; FIA, *Submission 3*, p. 9.

73 Office of the Privacy Commissioner, New Zealand, *Guidelines for Business, Frequently Asked Question*, p. 3, at: http://www.privacy.org.nz/comply/The%20Privacy%20Act%20And%20Your%20Business.pdf (accessed 9 June 2005).

74 See, for example, Caroline Chisholm Centre for Health Ethics, *Submission 21*, p. 12; Dr Anthony Place, *Submission 22*, p. 4; EFA, *Submission 17*, pp 34-35.

75 *Submission 17*, p. 34.

> …many small businesses, and individuals dealing with them, are uncertain as to whether or not the businesses are subject to the law.[76]

4.48 The APF further argued that:

> Some of the most privacy intrusive activities are carried out by very small companies and even sole traders – examples include private detectives, debt collectors, internet service providers and dating agencies.[77]

4.49 Similarly, the FIA argued that small businesses such as Internet services providers may hold significant personal information.[78] EFA suggested, at the very least, small businesses involved in the telecommunications and Internet services sector should be required to comply with the NPPs.[79]

4.50 The ALRC suggested that the exemption should be expanded to cover small businesses holding health information (including genetic information).[80] The ALRC noted that one of the exceptions to the small business exemption includes an organisation providing a health service, which holds information. However, the ALRC submitted that:

> …a small business that is not a health service provider nevertheless can remain exempt from the Act, even though it may hold health information—such as where a business stores genetic samples or acts as a genetic data repository, but does provide a health service…The ALRC is concerned that this loophole poses a potential risk to the privacy of both the individual concerned and his or her genetic relatives. *Essentially Yours* recommended that all small business operators that hold genetic information should be subject to the provisions of the Privacy Act, whether or not they provide a health service.[81]

4.51 On the other hand, the Australian Chamber of Commerce and Industry (ACCI) argued that large costs would be imposed if the small business exemption were removed. The ACCI argued that the turnover threshold in the small business exemption should be raised from $3 million to $5 million.[82] In contrast, the FIA argued that 'costs of compliance are not sufficient reason to grant exemption from the provisions of the Act.'[83]

---

76 *Submission 32*, p. 14.

77 *Submission 32*, p. 14.

78 *Submission 3*, p. 9.

79 *Submission 17*, p. 35.

80 *Submission 18*, p. 4.

81 *Submission 18*, p. 4.

82 *Submission 25*, pp 4-7.

83 *Submission 3*, p. 9.

4.52 The APF supported a lower threshold, preferably based on the number of employees:

> If there is to be a residual size threshold, we submit that $3 million pa turnover is far too high – businesses with this turnover are hardly 'small' in most peoples' eyes. We strongly suggest that any residual exemption threshold be more consistent with that used in analogous jurisdictions – for example the NSW Anti-Discrimination Act 1977 uses a threshold of 5 employees. While no more related to privacy risk than turnover, a number of employees threshold would at least be familiar to many businesses and somewhat more transparent to consumers.[84]

4.53 EFA disagreed with this approach:

> We are opposed to an exemption based on number of employees because this would still result in exemption for organisations that collected and disclose substantial amounts and types of personal information.[85]

4.54 After reviewing arguments for and against the small business exemption, and options for reform, the OPC review made three recommendations relating to the small business exemption. The OPC review recommended that the Attorney-General should consider making regulations under section 6E of the Privacy Act to prescribe small businesses in the tenancy databases and telecommunications sectors, including Internet service providers and public number directory producers, to ensure that they are covered by the Privacy Act.[86] As the Privacy Commissioner, Ms Karen Curtis, explained:

> I have also suggested that with those smaller businesses that are higher risk, and I have specifically mentioned internet service providers—tenancy database operators, for instance—the existing regulation-making power under the act be exercised to ensure that they are covered under the Privacy Act. At the moment there is some suggestion that some may not be. Internet service providers hold a lot of personal information about individuals and they of course are covered under the Telecommunications Act. That goes again to one of the problems with national consistency. Under the telco act they are covered; under the Privacy Act maybe they are not.[87]

4.55 The OPC review also recommended that the Australian Government consider amending the Privacy Act to remove the consent provisions in subsections 6D(7) and 6D(8).[88] The OPC review explained:

> Small businesses that trade in personal information are not exempt from the operation of the Privacy Act. If, however, the individual consents to the

---

84 *Submission 32*, pp 14-15.

85 *Submission 17*, pp 34-35.

86 OPC review, Recommendation 52, p. 185. See also Recommendations 9 and 15.

87 *Committee Hansard*, 19 May 2005, p. 48.

88 OPC review, Recommendation 53, p. 185.

> collection or disclosure of the personal information then the business remains a small business and is exempt [see sections 6D(7) and 6D(8)].[89]

4.56 As the OPC review remarks:

> 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.[90]

4.57 Finally, the OPC review recommended that:

> 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 [Australian Bureau of Statistics] definition, currently 20 employees or fewer, rather than annual turnover.[91]

4.58 As Ms Karen Curtis, the Privacy Commissioner, explained to the committee:

> I have recommended that the small business exemption be retained but modified. At the moment the small business operator is defined by turnover of $3 million. That is a bit cumbersome for everybody: for an individual who wants to know whether the person they are dealing with would be covered by the Privacy Act or not; for the business itself that is not quite aware where its turnover is; and for our office, when we are asked to investigate to establish whether there is jurisdiction, it is a little more complex than it needs to be when we look at turnover. I have suggested that the act be amended so that the definition relates to the number of employees, and I have suggested that the ABS definition, which is 20 employees, be used. I think it makes it easier for small business because that one is used more often in that area. [92]

4.59 In response to the committee's questions as to whether the small business exemption should be removed altogether, Ms Curtis replied:

> One of the premises of the [A]ct is that there be a balance between the individual's right to privacy and the community's needs, and between the free flow of information and businesses operating efficiently. If the small business exemption were removed entirely, there would be a cost to I think it is 1.2 million small businesses in Australia.[93]

---

89 OPC review, p. 185.

90 OPC review, p. 185.

91 OPC review, Recommendation 51, p. 185.

92 *Committee Hansard*, 19 May 2005, p. 48.

93 *Committee Hansard*, 19 May 2005, p. 49.

4.60 However, Ms Curtis acknowledged that the OPC had not made an assessment to estimate the actual cost of removing the small business exemption.[94]

4.61 APF supported this recommendation, but felt that the threshold should be lower, at the level of around five employees, consistent with anti-discrimination legislation.[95] However, APF also noted that:

> …privacy risks are contextual, rather than created or heightened simply by the size of the business. Some of the most privacy intrusive activities are carried out by very small companies and even sole traders.[96]

Media exemption

4.62 The media exemption in subsection 7B(4) of the Privacy Act also received some attention during the committee's inquiry. Subsection 7B(4) provides that acts done, or practices engaged in, by a media organisation is exemption from the Privacy Act if the act or practice is:

- by the organisation in the course of journalism; and
- at a time when the organisation is publicly committed to observing published standards that deal with privacy in the context of the activities of the media organisation.

4.63 The rationale for the media exemption was explained during the second reading speech to the Privacy Amendment (Private Sector) Bill 2000 as follows:

> The media in Australia have a unique and important role in keeping the Australian public informed. In developing the Bill, the government has sought to achieve a balance between the public interest in allowing a free flow of information to the public through the media and the individual's right to privacy.[97]

4.64 The Australian Press Council (APC) noted in its submission that it administers approved Privacy Standards for the print media under the media exemption in the Privacy Act. The APC submitted that: 'all major newspaper publishers' now subscribe to these standards; the media exemption is 'working effectively'; and the exemption strikes an 'appropriate balance between the flow of information of public interest and concern and individuals' rights to privacy in their

94 *Committee Hansard*, 19 May 2005, p. 49.

95 *Submission 32B*, p. 6.

96 *Submission 32B*, p. 5.

97 The Hon Daryl Williams AM QC MP, former Attorney-General, *House of Representatives Hansard*, 12 April 2000, p. 15752.

private affairs.'[98] The APC further pointed that it received a very low number of complaints in relation to invasion of privacy.[99]

4.65 Other organisations also expressed support, or at least, no opposition to, the current media exemption.[100] For example, the FIA felt that the exemption enables the 'free flow of information.'[101]

4.66 In contrast, the AMA suggested that the current media exemption should be reviewed, and that the media should be 'subject to privacy law when dealing with the personal health information of individuals, subject to appropriate exemptions to ensure that the public interest is properly served.'[102] The AMA was particularly concerned about protecting patients from exposure to the media, and provided examples of problems that had been encountered by mental health service providers.[103]

4.67 The APF was also critical of the media exemption. The APF submitted that 'media organisations can and do, all too frequently, seriously intrude into individuals' privacy without adequate justification.'[104] It argued that the exemption and the definition of 'media organisation' are far too wide and:

> …effectively allow any organisation to claim exemption from the Act for information which is 'published'. This weakness is compounded by the failure to define 'journalism'. The only constraint on organisations claiming this exemption is the condition of committing to published media standards, but as there are no criteria for these standards, or provision for review of them, the condition is effectively worthless.[105]

4.68 The APF further argued that:

> 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. However, the Foundation has always accepted that application of privacy principles to the media raises some special issues and that there needs to be a balance to reflect the public interest role of some media organizations.[106]

---

98 *Submission 8*, pp 1-2.

99 *Submission 8*, p. 4.

100 See, for example, FIA, *Submission 3*, p. 9; ACA, *Submission 15*, p. 4.

101 *Submission 3*, p. 9.

102 *Submission 9*, p. 12.

103 *Submission 9*, p. 12.

104 *Submission 32*, p. 13.

105 *Submission 32*, p. 13.

106 *Submission 32*, p. 13.

4.69 The APF suggested that an independent review and inquiry into the media and privacy should be conducted. In the short term, it suggested that the media exemption should be amended to 'focus more narrowly on the bona fide public interest media role of news and current affairs'. Finally, the APF suggested that the exemption should only apply on:

> …condition that (a) the privacy standard is a bona fide attempt to protect privacy from media intrusions (assessed as such by an independent arbiter – perhaps the Privacy Commissioner); (b) is enforced in some effective way; and (c) is generally observed by the media organisation concerned.[107]

4.70 The OPC review considered the media exemption and noted that the OPC receives very few inquiries and complaints about media organisations.[108] The Issues Paper released as part of the review suggested the current exemption 'may therefore strike an appropriate balance between privacy and the desirable free flow of information.'[109]

4.71 However, during this inquiry, the APF observed that:

> The low level of enquiries and complaints in this area cannot be taken as implying satisfaction – it is probably explained by a widespread and correct view that media are effectively above the law in relation to privacy.[110]

4.72 The OPC review recommended 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. [111]

4.73 The OPC review also noted that the OPC:

> …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.[112]

---

107 *Submission 32*, p. 13.

108 OPC review, p. 197.

109 OPC review, p. 195.

110 *Submission 32*, p. 13.

111 OPC review, Recommendation 58, p. 199.

112 OPC review, Recommendation 59, p. 197.

Employee records

4.74 Subsection 7B(3) of the Privacy Act also exempts acts or practices of employers relating to employee records.[113] The rationale for the employee records exemption was explained by the then Attorney-General in the second reading speech to the Privacy Amendment (Private Sector) Bill 2000:

> While this type of personal information [employee records] is deserving of privacy protection, it is the government's view that such protection is more properly a matter for workplace relations legislation.[114]

4.75 Several submissions were critical of the employee records exemption in the Privacy Act, and many of these suggested the exemption should be removed and/or reconsidered.[115] For example, the Centre for Law and Genetics argued that 'for the majority of workers in Australia there is little tangible protection of the privacy of their employment records.'[116] The Centre also argued that at both state and Commonwealth level, 'the current coverage of employee privacy in the workplace relations context is minimal and patently inadequate'.[117]

4.76 Similarly, Professor Weisbrot of the ALRC observed:

> …the intention was eventually to cover somewhere the privacy aspects of employee records. The government expressed a preference to deal with it in workplace relations. That has not happened yet. Our preference, after studying the area, in any event, would be to give it the same sort of protection that is accorded more generally under the Privacy Act.[118]

4.77 Professor Weisbrot further argued:

> We have difficulty seeing exactly how you would do that in the Workplace Relations Act. I think you would have to add a whole new division, which would substantially replicate what you already have in the Privacy Act, and it is unclear to us why you would do that, although it is technically possible.[119]

---

113 'Employee records' are then defined in section 6 of the Privacy Act.

114 The Hon Daryl Williams AM QC MP, Attorney-General, Second Reading Speech, *House of Representatives Hansard,* 12 April 2000, p. 15752.

115 See, for example, Anti-Discrimination Board of NSW, *Submission 12*, p. 7; CCHE, *Submission 21*, p. 12; Centre for Law and Genetics, *Submission 24*, p. 7, and Attachment 4; APF, *Submission* 32, pp 12-13; Correspondence from Dr Jocelynne A. Scutt, 24 May 2005; Professor Don Chalmers, Centre for Law and Genetics, *Committee Hansard*, 20 May 2005, p. 8. See also Professor Margaret Otlowski, 'Employment Sector By-Passed by the Privacy Amendments' (2001) 14 *Australian Journal of Labour Law*, 169-176.

116 *Submission 24*, Attachment 4, p. 38.

117 *Submission 24*, Attachment 4, p. 39.

118 *Committee Hansard*, 19 May 2005, p. 38.

119 *Committee Hansard*, 19 May 2005, p. 38.

4.78 The ALRC believed that the current provisions of the *Workplace Relations Act 1996* 'do not provide the scope to protect adequately the privacy of employee records.'[120] The ALRC noted the recommendation in the *Essentially Yours* report that the Privacy Act should be extended to cover genetic information contained in employee records, and that further consideration be given to other forms of personal health and medical information contained in employee records.[121] Professor Weisbrot explained:

> At the moment there is really no regulation of the right of an employer to hold that information or to ask for that information…we think as a general rule employers should not be asking for or using predictive health information in making decisions about employment.[122]

4.79 Professor Weisbrot also observed that:

> Interestingly enough, earlier on the groups that represent employers, particularly the ACCI, said that they did not want any alteration to the existing regime in respect of employment records, but by the end of the inquiry they acknowledged in their submission that they thought this was such a sensitive area that they would accept the amendment of the Privacy Act to cover genetic information at least in relation to employment records.[123]

4.80 The Anti-Discrimination Board of NSW was also concerned that the employee records provisions were unclear as to whether information obtained in the process of engaging employees may be caught by the employee records exemption.[124]

4.81 The Victorian Privacy Commissioner urged the committee to 'rethink the employee records exemption and to think in a holistic way about workplace privacy.'[125] Indeed, several submitters raised workplace privacy and workplace surveillance as an area where state and territory governments have begun legislating, and some argued that this was a response to the lack of regulation at the Commonwealth level.[126] For example, the APF pointed out that:

> The handling of personal information in the employment context is one of the areas in which protection is most needed, and the vacuum created by this exemption is already being partially filled by State government

---

120 *Submission 18*, p. 7.

121 *Submission 18*, p. 7; see also Professor David Weisbrot, ALRC, *Committee Hansard*, 19 May 2005, p. 38; and Centre for Law and Genetics, *Submission 24*, p. 7.

122 *Committee Hansard*, 19 May 2005, p. 38.

123 *Committee Hansard*, 19 May 2005, p. 38; see also ALRC, *Submission 18*, p. 7.

124 *Submission 12*, p. 7; see also AEIA, *Submission 16*, pp 1-2.

125 *Committee Hansard*, 22 April 2005, p. 13.

126 See, for example, Mr Bill O'Shea, LIV, *Committee Hansard*, 22 April 2005, p. 22; Mr Paul Chadwick, Victorian Privacy Commissioner, *Committee Hansard*, 22 April 2005, p. 13; see also ANZ, *Submission 6*, p. 5.

> initiatives on workplace privacy, further complicating the regulatory environment, which is in no-one's interests.[127]

4.82 Indeed, the OPC review of the privacy sector provisions recommended that:

> 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.[128]

4.83 As noted earlier in this chapter, the employee records exemption was excluded from the OPC review of the private sector provision on the grounds that it was already being reviewed under a separate process. However, the APF commented on the exclusion of the employee records exemption from the OPC review as follows:

> The government's 'excuse' that the employee record exemption is already under separate review might carry more weight if that other review were not being conducted effectively in secret, with no submissions having been published and no progress reported for almost twelve months.[129]

4.84 Indeed, the committee notes that the Attorney-General's Department's own fact sheet on the Privacy Act and employee records states:

> The Government will review existing Commonwealth, State and Territory laws to consider the extent of privacy protection for employee records and whether there is a need for further regulation. The review, which will be carried out by officers of the Attorney-General's Department and the Department of Employment, Workplace Relations and Small Business, will involve consultation with State and Territory Governments, the Privacy Commissioner and other key stakeholders. The review will be completed in time to assist the Privacy Commissioner when he conducts a more general review of the legislation two years after it commences operation.[130]

4.85 The OPC noted that it was awaiting the outcome of this review and that its submission to the review had supported the removal of the exemption from the Privacy Act. The OPC submitted that bringing employee records under the jurisdiction of the Privacy Act could:

> …provide greater consistency of coverage across public and private sector workplaces, and bring federal privacy legislation in line with other privacy law that protects private sector employee records (for example, the

---

127 *Submission 32*, pp 12-13; see also Mr Bill O'Shea, Law Institute of Victoria, *Committee Hansard*, 22 April 2005, p. 22.

128 OPC review, Recommendation 4, p. 48

129 *Submission 32*, p. 13.

130 Attorney-General's Department Fact Sheet on Privacy in the Private Sector, *Employee Records*, 22 December 2000, at: http://www.ag.gov.au/agd/WWW/agdHome.nsf/Page/Privacy_Law_Private_Sector_Fact_sheets_Employee_Records (accessed 3 June 2005).

> Victorian Health Records Act 2002). This step could bring greater clarity, particularly for employers, in relation to their information-handling obligations and the extent of protection for personal information in employee records.[131]

Political acts and practices

4.86 Section 7C of the Privacy Act provides an exemption for certain political acts and practices. The rationale for this exemption was explained by the then Attorney-General in the second reading speech to the Privacy Amendment (Private Sector) Bill 2000:

> Freedom of political communication is vitally important to the democratic process in Australia. This exemption is designed to encourage that freedom and enhance the operation of the electoral and political process in Australia.[132]

4.87 Several submissions were very critical of this exemption.[133] The Victorian Privacy Commissioner, Mr Paul Chadwick, expressed his view on this exemption at the committee's hearing in Melbourne:

> …there is a deep literature about public trust in public institutions. One aspect of trust is the willingness to submit to the same levels of accountability as everybody else, particularly the ones you impose on everyone else. I think that the political parties' exemption needs attention because of that.[134]

4.88 Mr Chadwick continued:

> There are mechanistic reasons why it needs attention—for example, the sophistication of the databases that your different party organisations maintain. They are often full of fine-grain data about the community, which you legitimately need, I think, to run a democratic community properly, to fight tightly fought election campaigns in marginal electorates and all the rest. … But you need to be much more open about what you do. I think you need to apply to yourselves two basic principles: you have to be more transparent about it, and you have to let people see what you hold about them and correct it if it is wrong.[135]

4.89 Mr Chadwick concluded that:

---

131 *Submission 48*, p. 7.

132 The Hon Daryl Williams AM QC MP, Attorney-General, Second Reading Speech, *House of Representatives Hansard*, 12 April 2000, p. 15752.

133 See for example, AMA, *Submission 8*, p. 13.

134 *Committee Hansard*, 22 April 2005, p. 9.

135 *Committee Hansard*, 22 April 2005, p. 9.

> It would be good for the credibility of the parliament and the political process if all the parties would address this question of your preferential treatment under the Privacy Act.[136]

4.90 The AMA suggested that the exemption for political organisations should be tightened, arguing that 'politicians can and do invade the privacy of individuals'.[137] The AMA gave an example of a federal politician who allegedly gained access to a woman's medical records against her wishes and then used these for political purposes.[138]

4.91 The APF went further in its criticism of the political acts and practices exemption, describing the exemption as 'unconscionable and hypocritical', arguing that:

> The government cannot morally and ethically justify exempting politicians and political parties from the privacy protection rules which have been applied to the rest of the community. We urge members of the Committee to set aside any self interest in leaving themselves outside the Privacy Act regime, and to take the only principled approach of recommending the removal of this exemption. There may be a need for modified rules to recognise the public interest in the democratic process, but the starting point should be a level playing field with equivalent standards.[139]

4.92 Ms Anna Johnston of the APF suggested that the exemption should be abolished, arguing that:

> Increasingly we believe that political parties operate as large corporations. Again it is an issue of having a level playing field. Other large corporations are subject to the Spam Act, subject to the direct marketing provisions and subject to all the privacy principles that political parties are not. We have seen recently a complaint about the allegation that there were direct marketing calls made to silent home telephone numbers. The complaint could not progress very far because ultimately the Privacy Commissioner concluded she had no jurisdiction. That complaint has faltered. I think that is a graphic illustration of where the exemption causes privacy difficulties.[140]

4.93 EFA also strongly objected to the exemption for political acts and practices, arguing that it should be deleted because:

> Political parties should be treated no differently from any other organisation in respecting the privacy rights of Australian citizens. To do so is to send a

---

136 *Committee Hansard*, 22 April 2005, p. 9.

137 *Submission 9*, pp 12-13.

138 *Submission 9*, p. 13.

139 *Submission 32*, p. 13.

140 *Committee Hansard*, 19 May 2005, p. 20; see also Mr David Vaile, APF, *Committee Hansard*, 19 May 2005, p. 20.

> message that the Privacy Act is only a token gesture, to be evaded when it happens to suit particular vested interests with the political clout to get their own way.[141]

4.94 EFA expressed particular concern that the exemption:

> …allows political parties to collect information about citizens from third parties that could be completely wrong, and does not even grant citizens a right to know what that information is and have it corrected if it is not true.[142]

4.95 In response to the committee's questions, the OPC noted that it had received relatively few complaints and inquiries relating to political acts and practices.[143] For example, the Deputy Privacy Commissioner, Mr Timothy Pilgrim replied:

> In the financial year 2003-04, we closed three complaints on the basis that they were exempted by the political exemption. In regard to that seemingly being a very low number, if people ring in and inquire about whether they should lodge a complaint, if it sounds on the face of it over the phone and we can determine it, we would tell the individual that there is a political exemption and more than likely we would not be able to investigate. I have just done a quick look at the numbers, and we had about 20 phone inquiries in the current financial year in regard to the political exemption.[144]

4.96 The Privacy Commissioner, Ms Karen Curtis, also observed that:

> …from 21 December 2001 when the legislation came into effect to 31 January 2005, we closed 24 per cent of total complaints—and there were 3,575 of those—as being out of jurisdiction. On the pie chart below 0.4 per of that 24 per cent, which is 24 per cent of 3,575, were political exemption.[145]

4.97 Again, as mentioned earlier in this chapter, the political acts and practices exemption was excluded from OPC review of the private sector provisions of the Privacy Act. The justification for that exclusion was that this and other exemptions had been subject of separate review. In response to the committee's questions as to what review was being, or had been, undertaken in relation to the political acts and practices exemption, the Attorney-General's Department answered:

> The review of the 2001 election by the Joint Standing Committee on Electoral [M]atters considered access by political parties to the electoral

---

141 *Submission 17*, pp 35-36.

142 *Submission 17*, p. 35.

143 *Submission 48*, p. 10.

144 *Committee Hansard*, 19 May 2005, p. 57.

145 *Committee Hansard*, 19 May 2005, p. 58.

> roll. The Department is not aware of any review that has considered the exemption for political acts and practices.[146]

Direct marketing

4.98 Some submissions were critical of the provisions of the Privacy Act which allow the use and disclosure of personal information for direct marketing in some circumstances.[147] For example, EFA suggested that the direct marketing provisions in the Privacy Act need a 'complete overhaul'.[148] The Victorian Privacy Commissioner, Mr Paul Chadwick, also observed the high level of public irritation with direct marketing, observing that:

> …people get so cross when telemarketers ring them at dinnertime: they feel they have left their life as a consumer at the front door and now they are doing something else. This is certainly the feeling that a privacy commissioner gets as he goes around the country, as he must, addressing the public. They are the single most asked questions: how did they get my number and why are they allowed to call me at dinnertime and address me by my first name.[149]

4.99 Indeed, the OPC review of the private sector provisions noted its research into community attitudes towards privacy (see discussion in chapter 2) had revealed that:

> 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).[150]

4.100 On the other hand, the ADMA, representing the direct marketing industry, cautioned that:

> …whilst for example, 46% of respondents to the OFPC research stated that organisations should not be able to collect information from telephone directories, individuals provide a different response when the question is asked in context. For example, the results of ADMA research show that Australians do see value in organisations collecting and using publicly available information for purposes such as product recall, data validation and database updating.[151]

---

146 *Submission 49*, p. 1.

147 See, for example, Ms Mary Lander, *Submission 19*, p. 1; EFA, *Submission 17*, p. 37; APF, *Submission 32*, p. 19; Mr Roger Clarke, *Submission 28*, p. 8.

148 *Submission 17*, p. 36.

149 *Committee Hansard*, 22 April 2005, p. 2.

150 OPC review, p. 96.

151 *Submission 38*, p. 12.

4.101 The ADMA further noted that its own research showed that:

> 80% of respondents are comfortable with organisations collecting and using personal information for direct marketing purposes if, within the first marketing communication and at any time subsequently, they are provided an opportunity opt-out. [152]

4.102 Direct marketing is provided for in NPP 2.1, which deals with the use and disclosure of personal information for a secondary purpose, including direct marketing.[153] NPP 2.1 distinguishes between primary and secondary purposes of the collection of personal information.

4.103 Under NPP 2.1(a), if an organisation collects information for the *primary* purpose of direct marketing, that organisation can use and disclose that information for that purpose. In addition, an organisation can use and disclose information for direct marketing if direct marketing is related to the primary purpose of collection, and the individual would reasonably expect the organisation to use or disclose the information for direct marketing purposes.[154]

4.104 EFA noted that if personal information is collected for the primary purpose of direct marketing, no consent is required. EFA suggested that the NPPs should be amended to prohibit collection of personal information without consent for the 'primary purpose' of direct marketing.[155]

4.105 Miss Jodie Sangster of the ADMA also commented on this issue:

> It seems that there is a gap in the legislation there in that if you indirectly collect data for the primary purpose of direct marketing then there is currently no requirement to give that individual an opportunity to opt out of receiving anything further. So we have suggested that, where data is collected not from the individual, in the first marketing approach there should be something expressly in there that says, 'If you don't wish to receive further marketing, please let us know.' It should tell the individual how to do that. That obviously would be backed up by this right for the individual to be able to opt out at any time.[156]

---

152 *Submission 38*, p. 15.

153 See further Attorney-General's Department Fact Sheet on Privacy in the Private Sector, *Direct Marketing*, 22 December 2000, at: http://www.ag.gov.au/agd/WWW/agdHome.nsf/Page/Privacy_Law_Private_Sector_Fact_sheets_Direct_Marketing (accessed 5 May 2005); or OPC review, pp 94-95.

154 See further Attorney-General's Department Fact Sheet on Privacy in the Private Sector, *Direct Marketing*, 22 December 2000, at: http://www.ag.gov.au/agd/WWW/agdHome.nsf/Page/Privacy_Law_Private_Sector_Fact_sheets_Direct_Marketing (accessed 5 May 2005); or OPC review, pp 94-95.

155 *Submission 17*, p. 36.

156 *Committee Hansard*, 19 May 2005, p. 31.

4.106 NPP 2.1(c) provides for the use of information for the *secondary purpose* of direct marketing. An organisation can also use personal information for direct marketing in certain circumstances, even if direct marketing was not the primary purpose of collection, or the direct marketing is unrelated to the purpose of collection and not within the reasonable expectations of the person who 'owns' the information. However, there are some criteria that must be met before an organisation may use or disclose the information for the *secondary purpose* of direct marketing. For example, in every communication, the organisation must give the individual the opportunity to opt-out of receiving further direct marketing communications.[157]

4.107 EFA expressed the view that 'the NPP 2.1(c) exception permitting secondary use of personal information for direct marketing without consent is totally unacceptable.' EFA argued that:

> Personal information should only be used for marketing purposes with explicit consent, not by default with the blessing of the government. Unsolicited direct marketing, whether in the form of junk mail, telemarketing phone calls, junk fax or by E-mail is notoriously unpopular with consumers.[158]

4.108 EFA further emphasised that:

> The direct marketing exemption requires a consumer to be aware that they are permitting the use of their data (provided for the primary purpose of, e.g. purchasing a specific product) to also be used for the secondary purpose of direct marketing unless they remember to specifically request not to receive direct marketing communications at the time of providing the information.[159]

Opt in or opt out?

4.109 Several submissions recommended that the direct marketing exceptions in NPP 2.1 be replaced with an 'opt-in' provision that permits the use of personal information for direct marketing purposes only with specific prior consent.[160]

4.110 In particular, a number of submissions suggested that, in relation to direct marketing, the Privacy Act should be brought into line with the *Spam Act 2003*. For example, EFA pointed out that the direct marketing exception in the Privacy Act is inconsistent with the *Spam Act 2003*, in that it permits sending of messages without

---

157 See further Attorney-General's Department Fact Sheet on Privacy in the Private Sector, *Direct Marketing*, 22 December 2000, at: http://www.ag.gov.au/agd/WWW/agdHome.nsf/Page/Privacy_Law_Private_Sector_Fact_sheets_Direct_Marketing (accessed 5 May 2005); or OPC, Privacy Commissioner report, pp 94-95.

158 *Submission 17*, p. 36.

159 *Submission 17*, pp 36-37.

160 See, for example, EFA, *Submission 17*, p. 37; APF, *Submission 32*, p. 19; Mr Roger Clarke, *Submission 28*, p. 8; Consumer Credit Legal Centre (NSW), *Submission 35*, p. 3.

consent. EFA argued that, as a minimum, NPP 2.1(c)(i) should be amended to be equivalent to the Spam Act in relation to consent.[161]

4.111 Similarly, the APF also pointed to the *Spam Act 2003*, arguing that:

> In our view, the level of public irritation with direct marketing, and the general lack of awareness and understanding of marketing methods, justify a simple across the board requirement for prior consent (opt-in). This could be based on the Spam Act model which allows for either express on inferred consent, although we suggest that the ACA guidance on inferred consent allows for practices which would be outside the reasonable expectation of most consumers, and this aspect of an opt-in regime should be tighter.[162]

4.112 Ms Anna Johnston gave a recent example of the first successful prosecution in Australia under the *Spam Act 2003*, where the company involved pleaded guilty, but:

> …made the point that their competitors could nonetheless call their customers using the telephone and not be subject to the same rules. Partly, in business terms it is about a level playing field between the means of technology. Obviously, the bigger players can afford telephone calls and the smaller players look to rely on email and SMS. They were not actually calling for the Spam Act to be changed but for the playing field to be level so that everyone is working on an opt-in basis.[163]

4.113 However, the ADMA disagreed with the suggestion of bringing the Privacy Act in line with the *Spam Act 2003*:

> That is not a move that our membership supports. We do believe that the Privacy Act is really around the use of data—it is not about regulating channels—and the Spam Act is about regulating the use of a channel. So, for that reason, we do not believe that they should be brought into line with each other. The other point is that with regard to something like direct mail—which is quite different from receiving, say, an SMS message—the level of intrusion is quite different. So a consumer who receives direct mail, providing they are given an opportunity to opt out, is given adequate protection there, whereas it is obvious with something like a text message, which is an awful lot more personal and a lot more intrusive, that further protection is needed.[164]

4.114 The ADMA strongly supported the continued inclusion of the direct marketing exemption in the Act. However, it did submit that it would support an 'opt-out' provision where organisations indirectly collect personal information for

---

161 See, for example, EFA, *Submission 17*, p. 36.

162 *Submission 32*, p. 19.

163 *Committee Hansard*, 19 May 2005, p. 15.

164 Miss Jodie Sangster, ADMA, *Committee Hansard*, 19 May 2005, p. 32.

unsolicited direct market purposes.[165] Miss Jodie Sangster from ADMA explained to the committee:

> …consumers should really have a right at any time to say to a company, 'I don't want to receive any further direct marketing from you.' Whereas currently they are given an opportunity right at the outset to say, 'I don't want my data used in this way,' I think it is fair to say that if consumers are receiving marketing that they are not finding is relevant to them then they should be able to go back at a later stage and say to that company, 'I don't want to receive this anymore. Can you please stop marketing to me.' Speaking to our member companies, that is already happening. If somebody does come back to them in that way then obviously the company does not want to marketing to them. It is not business efficient to be marketing to people who do not want to hear from you.[166]

4.115 For the APF, a requirement for all organisations to offer an opt-out with each direct marketing communication would be 'very much a second best amendment, but still better than the current position.'[167]

4.116 On the other hand, ANZ believed that the 'opt out provisions for customers to decline receiving marketing material from us are working well.' ANZ believed that it is premature to consider whether there is a need for a legislated opt out provision.[168] Similarly, Baycorp Advantage suggested that the current opt-out provisions are 'operating effectively' and argued that 'an opt-in regime would be unnecessarily obstructive of business'.[169] Nevertheless Baycorp Advantage suggested that:

> NPP 1.5 should be amended to increase the obligation on organisations acquiring personal information from third parties to advise consumers of opt-out rights at the first opportunity after acquisition (usually in the context of a direct marketing initiative) in line with current direct marketing industry practice.[170]

4.117 Mr Andrew Want from Baycorp Advantage elaborated on this during the committee's hearing in Sydney:

> In theory, while an opt-in regime, or for that matter an opt-out regime, provides consumers with control, the reality is that most consumers do not have any idea, I think, of what consents they have or have not given. A typical person with a car loan, a personal loan, a couple of bank loans and a mobile phone and a gas bill et cetera will have signed dozens and dozens of

165 *Submission 38*, p. 13.

166 *Committee Hansard*, 19 May 2005, p. 31.

167 *Submission 32*, p. 19.

168 *Submission 6*, p. 3.

169 *Submission 43*, p. 13.

170 *Submission 43*, p. 13.

> privacy consents with no way of knowing or remembering what they have signed when. The reality of control is probably a bit illusory.[171]

4.118 The FIA commented that a definition of direct marketing should be developed, in consultation with the fundraising industry, as it felt that this was an area of practice which is not entirely understood.[172]

Transparency

4.119 Some submitters suggested that organisations using direct marketing should be required to disclose the originating source of an individual's contact details.[173]

4.120 The Victorian Privacy Commissioner suggested more broadly that greater transparency could be achieved in the collection and handling of personal information by the public and private sectors, including greater notice about data sharing arrangements. In particular, the Victorian Privacy Commissioner pointed to recent 'shine the light' legislation in California in the US, which 'requires commercial entities to tell people what they are going to do with their personal information and who they give it to habitually'.[174] Mr Chadwick explained:

> It is an attempt to allow people to answer the question, 'How did you get my number?' They say, when the telemarketers ring at dinnertime, 'How do you know this number?' Sometimes they say: 'I have a silent number. Where did you get this?' The aim is to have more transparency. I think transparency is a greatly undervalued tool in this area of privacy—and that is partly because it is counterintuitive.[175]

4.121 The ADMA expressed qualified support for disclosure of the originating source of personal information in relation to unsolicited marketing material:

> …steps should be taken to gradually introduce a requirement for organisations that are using personal information to make unsolicited marketing approaches, on request from an individual, to inform the individual where the data was sourced.[176]

4.122 For example, Miss Jodie Sangster of the ADMA observed that:

---

171 *Committee Hansard*, 19 May 2005, p. 6.

172 *Submission 3*, p. 5.

173 See, for example, Ms Mary Lander, *Submission 19*, p. 1; see also Dr Anthony Place, *Submission 22*, p. 3.

174 Mr Paul Chadwick, *Committee Hansard*, 22 April 2005, p. 7; see also *Submission 33*, p. 5.

175 *Committee Hansard*, 22 April 2005, p. 7; see also *Submission 33*, p. 5.

176 *Submission 38*, pp 4 & 16.

> …if consumers receive an unsolicited approach from a company then a major concern to them is that they do not know where that company got their data from.[177]

4.123 Miss Sangster continued:

> What we have suggested is that, where a customer gets an unsolicited contact, the customer should have a right to ask, 'Where did you get my data from?' and the company that has made that contact should take reasonable steps to let the individual know where that data came from. That will allow the consumer then to go to that person and say, 'Can you please not pass my name out anymore.'…we have recommended that it be introduced as a guideline in the first instance…and then later on, once they have their systems in place, as a legal requirement.[178]

OPC review and direct marketing

4.124 The OPC review of the private sector provisions also considered the issue of direct marketing.[179] The review recommended that 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;
- 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; and
- exploring options for establishing a national 'Do Not Contact' register.[180]

Other issues in relation to the private sector provisions

Compliance with the EU directive and other international standards

4.125 As outlined in chapter 2 of this report, one of the objectives of the private sector provisions was to facilitate trade with the EU.[181] That is, to provide 'adequate' data protection standards under the EU Data Protection Directive to prevent restrictions on the transfer of information between EU and Australian companies.

---

177 *Committee Hansard*, 19 May 2005, p. 31.

178 *Committee Hansard*, 19 May 2005, p. 31.

179 OPC review, pp 94-103.

180 OPC review, Recommendations 23-25, p. 103.

181 See also Ms Karen Curtis, Privacy Commissioner, *Committee Hansard*, 19 May 2005, p. 48.

4.126 However, some submitters pointed out that the EU has not recognised Australia's privacy legislation as 'adequate'.[182] For example, the LIV argued that:

> Australia has not enacted legislation that protects privacy rights to the standard enjoyed in the EU, with the effect that the uncertainty that the legislation was intended to avoid continues to exist.[183]

4.127 Mr Bill O'Shea from the LIV explained further at the committee's hearing in Melbourne:

> In terms of business, our submission deals with the need for Australia to have a privacy system that complies with the EU directive. It is particularly important for Australian businesses that are collecting information and want to deal transnationally. If we do not comply with the EU directive, Australian businesses are going to be impacted in terms of the extent to which they can work offshore and deal with other jurisdictions. At the moment, our privacy regime does not meet the EU directive.[184]

4.128 The LIV noted that many of the inadequacies identified by the EU still exist in the legislation, and proposed that the Act should be amended to comply with the EU directive. In the LIV's view, some of the most significant concerns for the EU are the small business exemption and the employee records exemption. Other concerns raised by the LIV in this context included:

> - the width of the exception permitting an organisation to use or disclose personal information for a purpose for which the person has not consented if it is 'authorised' by another law to do so;
> - the exemption of data once it is publicly available;
> - the ability of organisations to notify people that their data has been collected, and why, after it has already been collected;
> - the ability to use and disclose information for direct marketing purposes, without the person's consent, if this was the primary purpose for which it was collected; and
> - the lack of special restrictions on the use and disclosure of sensitive information.[185]

4.129 Mr Bill O'Shea argued that:

> …we need to get our privacy protection regime in order so that there is no downstream problem—for example, for an Australian technology company

182 APF, *Submission 32*, pp 9-10; LIV, *Submission 37*, p. 8.

183 *Submission 37*, p. 9.

184 *Committee Hansard*, 22 April 2005, p. 15.

185 *Submission 37*, pp 8-9.

> wishing to do business in Europe and suddenly finding that they do not comply and that therefore the data cannot be transferred.[186]

4.130 On the other hand, the ADMA submitted that although Australia's privacy regime has not been recognised as 'adequate' by the EU, this had not hindered the ability of organisations to conduct business with European counterparts.[187] Similarly, the Privacy Commissioner, Ms Karen Curtis, observed that, in practice, businesses have been able to cope with the fact that EU adequacy has not been achieved by including relevant privacy standards in contracts:

> They have used contractual provisions to help them with transferring personal information overseas and dealing with European countries.[188]

4.131 Nevertheless, the LIV argued that there were potential flow-on effects as a result of the lack of EU recognition:

> …one of the subsequent issues is the current push for various free trade agreements in Asia. The standards of data protection in Asia are considerably lower than they are in the EU. One of the consequences of that is that if Australian companies, for example, were to put call centres or other operations into Asian countries, the personal information held in those centres would be subject to standards that are arguably lower than in Australia and vastly lower than in the EU. So there are issues in terms of not only Australia's involvement or Australia's privacy regime vis-a-vis the EU, but also indeed in terms of our Asian trading partners, whom we are now rapidly signing up to these agreements with.[189]

4.132 In a related issue, several submissions noted that Asia-Pacific Economic Cooperation (APEC) had also recently adopted a privacy standards framework.[190] For example, the APF submitted that while the APEC framework:

> …could provide a useful stimulus to privacy protection in other countries in our region, it could also potentially be used as an excuse to undermine existing levels of protection in countries such as Australia.[191]

---

186 *Committee Hansard*, 22 April 2005, p. 21.

187 ADMA, *Submission* 38, p. 7; see also Miss Jodie Sangster, ADMA, *Committee Hansard*, 19 May 2005, p. 36.

188 Privacy Commissioner, *Committee Hansard*, 19 May 2005, p. 48.

189 *Committee Hansard*, 22 April 2005, p. 21.

190 See, for example, Victorian Privacy Commissioner, *Submission 33*, p. 2; LIV, *Submission* 37, p. 9; APF, *Submission 32*, p. 10; see also Asia-Pacific Economic Cooperation (APEC), APEC Privacy Framework, 2004/AMM/014rev1, endorsed by the 16th APEC Ministerial Meeting, Santiago, Chile, 17-18 November 2004, http://www.apec.org/apec/news___media/2004_media_releases/201104_apecminsendorseprivacyfrmwk.html (accessed 1 June 2005)

191 *Submission 32*, p. 10; see also *Submission 32*, Annexure C.

4.133 Ms Anna Johnston of the APF elaborated on this during the committee's hearing in Sydney, observing that:

> …there is also a project going on at the moment between the APEC economies to develop international standards for those countries. One of the Privacy Foundation's concerns about that is that one of the descriptions of the privacy principles is that it is a privacy-light regime and that the principles are heading for a lowest common denominator rather than a highest common denominator between those economies.[192]

4.134 In relation to the APEC framework, the OPC review stated:

> 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.[193]

4.135 The OPC review of the private sector provisions also considered the issue of adequacy under the EU Data Protection Directive. The OPC review noted that while Australian laws have not yet received EU adequacy, 'negotiations with the European Commission regarding the adequacy of the Privacy Act in meeting the EU Directive have been continuing.'[194] In particular, the review noted that the small business and employee records exemptions had been the subject of continuing discussions. The review concluded by recommending that:

> 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.[195]

4.136 In response to the committee's questions as whether it was still necessary or desirable to achieve EU adequacy in light of the fact that most businesses were using

---

192 *Committee Hansard*, 19 May 2005, p. 14.

193 OPC review, p. 75.

194 OPC review, p. 74; see also Ms Karen Curtis, OPC, *Committee Hansard*, 19 May 2005, p. 48.

195 OPC review, Recommendation 17, p. 76.

contractual provisions, the Privacy Commissioner replied that it would be simpler for business if they did not have to use contracts for privacy provisions.[196]

4.137 However, the APF was concerned that the OPC's discussions on the EU Data Protection Directive (and indeed the review more generally) had focussed too much on the impact on business, ignoring the implications for consumers:

> …the issue of the continued lack of EU acceptance of the Privacy Act is treated as an issue for business, such as by examining the impact on trade. The impact on consumers of international data exchange is virtually ignored, despite the significant risks for consumers posed by data export, data havens, and globalisation of business interests.[197]

4.138 In response to the committee's questions on this issue, representatives from the Attorney-General's Department noted that negotiations with the EU are continuing and that:

> …we are still negotiating with the European Union. There is increasing understanding on the part of the European Commission of how Australia's privacy laws work…The last contact we had with them was in October last year in relation to general adequacy for the Privacy Act, and they did not raise any new or significant objections. I think their view is that this is something that has been on their agenda for quite some time and they would quite like to have the situation resolved as well, and the commission view seems to be resolved in a positive way. We are talking to commission officials, not the commissioners themselves or data protection commissioners, and I think the prospects are good in the medium term.[198]

4.139 The Departmental representative noted that the small business exemption is 'probably the key outstanding issue' to be resolved between the Europeans and Australia.[199]

Bundled consent

4.140 Some submissions expressed concern about the use of 'bundled consent' in some circumstances. 'Bundled consent' refers to the practice of obtaining consent for a broad range of uses and disclosures in relation to personal information without giving the individual a chance to choose which uses and disclosures they agree to or not.[200] The APF and EFA expressed concern that this practice may be undermining the operation and objectives of the Privacy Act.[201] For example, EFA argued that:

---

196 *Committee Hansard*, 19 May 2005, p. 50.

197 *Submission 32B*, p. 2.

198 *Committee Hansard*, 19 May 2005, p. 63.

199 *Committee Hansard*, 19 May 2005, p. 63.

200 OPC, *Submission 48*, p. 16; see also OPC review, p. 82; APF, *Submission 32*, pp 18-19.

201 APF, *Submission 32*, p.18; EFA, *Submission 17*, pp 38-39.

> 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.[202]

4.141 Similarly, APF was concerned that:

> Individuals are commonly asked or required to sign off on a 'package' of uses and disclosures, at least some of which are nonessential for the transaction being entered into. Lack of awareness and/or understanding, together with an imbalance of power means that few consumers ever challenge such requests, but this should not be taken as indicating acceptance of a fundamentally privacy intrusive practice.[203]

4.142 In contrast, some submitters expressed support for the ability to 'bundle' consent.[204] For example, the FIA argued that it is essential to 'business efficiency.[205] The ADMA suggested that it would be 'impractical' for many organisations to require separate consent for each data use of disclosure.[206] Similarly, Baycorp Advantage submitted that:

> Practices such as bundled consent indisputably create more efficient processes for a wide range of businesses. Baycorp Advantage's business, as a specialist data processor, depends on its capacity to rely on indirect collection and bundled consent. The ability to cleanse and enhance data against publicly available information further enhances the ability of businesses to improve their knowledge of their customer base. Baycorp Advantage submits that an inability to obtain consent in this manner would have an unnecessarily burdensome impact on the ability of businesses to operate efficiently...[207]

4.143 Mr Chris Gration from Baycorp Advantage explained to the committee:

> We are not arguing to detract from a consent based regime; we do not want to dismantle it. What we are saying is that, in an information society where the volumes of data held keep increasing exponentially, to keep expecting that the regulatory regime will exist solely on a regime of individual consent is insufficient.[208]

4.144 The APF recognised that 'bundling' may be reasonable in some circumstances:

---

202 *Submission 17*, p. 38.

203 *Submission 32*, p. 18.

204 FIA, *Submission 3*, p. 7; ADMA, *Submission* 38, p. 10.

205 FIA, *Submission 3*, p. 7.

206 *Submission 38*, p. 10.

207 *Submission 43*, p. 14; see also Mr Chris Gration, Baycorp Advantage, *Committee Hansard*, 19 May 2005, p. 6 cf EFA, *Submission 17*, p. 41.

208 *Committee Hansard*, 19 May 2005, p. 7.

> …for example it is reasonable to reserve a right to investigate future claims when selling insurance. Such exceptions should be addressed with notice/acknowledgement of the secondary use as a condition of the initial transaction. However it should not be open to businesses to make consent for non-essential secondary uses a condition of doing business. The default position should be that clear separate consent is obtained for 'discretionary' secondary uses.[209]

4.145 In response to the committee's questions on this issue, the OPC noted that it had received 33 complaints relating to the issue of bundled consent since 21 December 2001.[210]

4.146 The OPC's review of the private sector provisions noted that the practice of bundled consent 'may confuse consumers and may derogate from their rights under the Act. It is also an issue that confuses a lot of organisations.'[211] The OPC noted that it could 'play a role in working with stakeholders to clarify the issue' and concluded by recommending that:

> 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.[212]

4.147 In response to the committee's questions on this issue, the OPC noted that the guidance is likely to include:

> • Clearing up any misconceptions about how the NPPs apply that may be contributing to unnecessary bundling of consent
>
> • Giving practical guidance on how to give individuals choice where it is most likely to be required by the NPPs and wanted by consumers.[213]

4.148 However, the APF expressed its disappointment at the OPC review's response to the issue of bundled consent:

> While the OFPC report identifies and extensively discussed these problems – and indeed we are pleased to note the OFPC has been vocal about this issue for some years now – we are greatly disappointed that the report makes no recommendations on how to address this problem. Instead, recommendations 19-21 focus on short forms of privacy notices. We feel that this is an inadequate response to an on-going problem of abuse of consent requirements by business.[214]

---

209 *Submission 32*, p. 19.

210 *Submission 48*, p. 17.

211 OPC review, p. 92.

212 OPC review, Recommendation 22, p. 93.

213 *Submission 48*, p. 18.

214 *Submission 32B*, p. 4; see also Ms Anna Johnston, APF, *Committee Hansard,* 19 May 2005, pp 20-21.

Costs of compliance with private sector provisions

4.149 The ACCI submitted that the issue of the costs of compliance with the privacy legislation in the private sector was 'critically important to the business community.' The ACCI believed that those costs are 'considerable' and suggested that an in-depth study should be commissioned to examine compliance costs for business.[215]

4.150 In contrast, the FIA advised that, while the fundraising industry incurs costs in complying with privacy law, 'the benefits to business, and Australian society, outweigh the costs of compliance.'[216]

4.151 The ACA submitted that it had 'little sympathy' with complaints about compliance costs with the privacy legislation. It pointed out that there is no required reporting and no mandatory recording.[217]

4.152 Legal Aid Queensland noted that a number of small not for profit organisations are required to comply with the private sector provisions, and that for these organisations, this has 'caused great disruption and significant commitment of limited resources in order to ensure compliance. Many of these organisations struggle to remain financially viable.'[218]

4.153 The OPC review of the private sector provisions discussed the issue of costs of compliance, but did not appear to make any direct conclusions or recommendations on the issue.[219]

4.154 The committee received little other evidence on this issue, with the exception of some discussion of compliance costs in relation to the small business exemption as discussed earlier in this chapter.

Approved Privacy Codes

4.155 Several submissions also raised the provisions in the Privacy Act for the approval of industry codes by the Privacy Commissioner.[220] Before such codes can be approved, the Privacy Commissioner must be satisfied, among other things, that the code incorporates all the NPPs or sets out obligations that, 'overall are at least the

---

215 *Submission 25*, p. 3.

216 *Submission 3*, p. 8.

217 *Submission 15*, pp 16-17.

218 *Submission 31*, p. 4.

219 OPC review, pp 171-175; see also Ms Karen Curtis, OPC, *Committee Hansard*, 19 May 2005, p. 49.

220 See Privacy Act, Part IIIAA. Concerns in relation to the use of codes of practice relating to particular technologies are outlined in the chapter on emerging technologies.

equivalent' of all the obligations set out in the NPPs.[221] The OPC has also developed guidelines on Privacy Code development.[222]

4.156 Although submissions were generally supportive of these codes, many observed that only a low number of codes had been approved under the Privacy Act to date. Some of these submissions speculated on the reasons why so few codes have been developed and approved.

4.157 The ACCI was supportive of the system of voluntary codes under the privacy legislation. It noted that only three codes have been approved to date, and speculated that a low number of approved codes could be viewed as a success rather than a failing.[223] For example, the ACCI observed in relation to the low number of approved codes that:

> Rather than stemming from a deficiency in the approval mechanism, ACCI would suggest this in part reflects the relative priority consumers place on privacy matters in dealing with business. Australian businesses generally have a good track record in terms of respecting the rights of their customers and as a result the demand for an increased standard is probably minimal.[224]

4.158 However, the ACCI concluded that 'more time will need to pass before a definitive conclusion can be drawn in relation to the efficacy of voluntary codes'.[225]

4.159 The FIA were strongly supportive of industry codes of practice sanctioned under the Act, arguing that this would increase public awareness and consumer confidence.[226] The Real Estate Institute of Australia also discussed industry codes, but concluded that 'alternative supporting mechanisms such as industry-specific guidelines on the Privacy Act would provide practical information for compliance by businesses.'[227]

4.160 The ADMA believed that the reasons for the low number of approved privacy codes included the complexity of the process, the expense and resources involved in developing such codes, and the requirement that codes embody higher (or at least equivalent) standards.[228]

4.161 The APF also noted the low number of approved codes:

---

221 Privacy Act, paragraph 18BB(2)(a).

222 Available at: http://www.privacy.gov.au/act/guidelines/index.html#3.1 (accessed 30 May 2005).

223 *Submission 25*, p. 7.

224 *Submission 25*, p. 7.

225 *Submission 25*, p. 7.

226 FIA, *Submission 3*, p. 8.

227 *Submission 1*, p. 2.

228 *Submission 38*, p. 14.

> There has been relatively little take up of the Codes option by the private sector. We do not find this surprising and have always been sceptical of the government's enthusiasm for the Code provisions. A Code cannot, overall, lower the standards of the NPPs and that is a critical feature that must remain. Given this, and the equally important feature that decisions of Code Adjudicators can be appealed to the Privacy Commissioner, there is little advantage to businesses in developing or adopting a Code. The Code development and approval process is, quite rightly, fairly lengthy and onerous, and if a Code includes a complaints handling process this is effectively privatising costs which under the default scheme are borne by the government.[229]

4.162 Similarly, Ms Irene Graham from EFA submitted:

> Virtually no industry codes have been developed at all. It has been said, I understand, in submissions to the Privacy Commissioner's inquiry and so forth that the basic reason that industries have not developed codes is that it is just too expensive and that to have a code they then need to have a complaints process and an adjudicator relative to their own code, so it all becomes exceedingly expensive for industry.[230]

4.163 The APF was further concerned that 'a proliferation of [c]odes would further confuse the public and detract from the already difficult task of building awareness of the Act and the Commissioner.'[231] The APF suggested some changes to code provisions, including that:

- codes should be disallowable by Parliament;
- the Privacy Commissioner should be able to initiate a code;
- the Privacy Commissioner should be required to make public the submission by a code proponent dealing with public consultation;
- the courts should be expressly deemed to have notice of codes in the Register kept by the Privacy Commissioner; and
- the Privacy Commissioner should be able to review any decision of a code adjudicator.[232]

4.164 As discussed in the previous chapter, the ACA raised concerns with the development of codes in relation to specific technologies, rather than industries.[233]

---

229 *Submission 32*, p. 21.

230 *Committee Hansard*, 22 April 2005, p. 47.

231 *Submission 32*, p. 21.

232 *Submission 32*, p. 22.

233 *Submission 15*, p. 1; see also Mr Charles Britton, ACA, *Committee Hansard*, 19 May 2005, p. 24.

4.165 The OPC review of the private sector provisions also considered the issue of approved privacy codes. The review noted the support for the codes, and that most submissions to that review focussed on simplifying the process for approval of codes. As the Privacy Commissioner, Ms Karen Curtis, explained to the committee:

> Another area where the original objective has not been met is the development of national privacy principle codes. To date, the office has only approved three codes, and business has not felt the need to adopt codes; it is complying with the law. Originally it was believed that codes would be adopted by business or business organisations. I have suggested as one of the recommendations that we may need to look within our office at reviewing our code development guidelines to make it simpler for business.[234]

4.166 The OPC review committed that the OPC would 'review the Code Development Guidelines dealing with the processes relating to code approval with a view to simplifying them.'[235] However, the APF was critical of this recommendation, expressing its view that:

> Codes add little value, diminish clarity in the law, and disperse accountability. Codes are no better than legislation that is not enforced.[236]

4.167 Further, the OPC review recommended that the Australian Government should consider amending the Privacy Act to provide for a power to make binding codes.[237] The OPC suggested this primarily as a way of 'overcoming problems caused by inconsistent state and territory legislation regulating a particular activity.'[238] The OPC noted that, for example, codes for a specific sector could be developed by the Privacy Commissioner following a request by the Attorney-General, or at the Commissioner's own initiative. The Privacy Commissioner, Ms Karen Curtis, explained to the committee the difference between codes under the existing provisions and the proposal for binding codes:

> The national privacy codes that businesses can develop must include all of the national privacy principles, or at least incorporate the equivalent standard of those NPPs. And then they have to have a code adjudicator process—all of those sorts of things. The idea of the binding codes that we have suggested is to come up in other areas where perhaps they were not going to be voluntary. The NPP codes are developed on a voluntary basis. The ones that were binding could possibly be done for technology, or for an

234 *Committee Hansard*, 19 May 2005, p. 48.

235 OPC review, Recommendation 47, p. 171; see also Ms Karen Curtis, OPC, *Committee Hansard*, 19 May 2005, p. 48.

236 *Submission 32B*, p. 5.

237 OPC review, Recommendation 7, p. 48.

238 OPC review, p. 47.

> industry that was not working as well—perhaps the tenancy database area.[239]

4.168 Mr Charles Britton of the ACA was supportive of this recommendation:

> Certainly one of the important things is the recommendation for the ability to make binding codes. I think that in part goes to the question of new technologies and suchlike. It is important for the codes not simply to be those of industry associations but to be able to be the Privacy Commissioner's and to be binding codes on people who use the technologies or participate in the industries. I think that is part of closing some of the gaps in the regulatory ladder, if you like, between self-regulation and legislation.[240]

Other aspects of the NPPs and private sector provisions

4.169 Many other issues, concerns and suggestions for amendments to the private sector provisions of the Privacy Act, and in particular specific aspects of the NPPs, were raised during this inquiry. There were also other, similar recommendations in the OPC review of the private sector provisions.[241] Unfortunately it is not possible to discuss all these issues in detail in this report.

4.170 For example, some submissions suggested that there should be greater controls on collection provisions of the NPPs.[242] APF and EFA proposed that the NPPs should expressly include a prohibition on collecting information known to be unlawfully disclosed.[243] The APF also pointed out that under Canadian federal privacy sector law, collection is allowed 'only for purposes that a reasonable person would consider are appropriate in the circumstances.'[244]

4.171 Some of the other issues and concerns raised included that:

- corporate privacy policies can be changed without notice;[245]
- 'use' under NPP2 should include access;[246]
- the anonymity provisions in NPP8 be strengthened;[247]

---

239 *Committee Hansard*, 19 May 2005, p. 49.

240 *Committee Hansard*, 19 May 2005, p. 27.

241 See, for example, OPC review, Recommendations 74-84.

242 See, for example, Ms Irene Graham, EFA, *Committee Hansard*, 22 April 2005, p. 41; EFA, *Submission 17*, pp 13-14.

243 APF, *Submission 32*, p. 15; EFA, *Submission 17*, p. 42.

244 *Submission 32*, pp 15-16; see also EFA, *Submission 17*, p. 38.

245 EFA, *Submission 17*, pp 39-40; APF, *Submission 32*, p 17, 18; see also OPC review, p. 84.

246 APF, *Submission 32*, p. 17.

247 EFA, *Submission 17*, p. 44; APF, *Submission 32*, p. 17.

- the exemption for private/personal use should be revisited;[248]
- publicly available personal information should not be exempt;[249]
- the exception for related bodies corporate (provided for in section 13B) should be deleted and they should be treated as third parties;[250]
- the secondary purpose exemption at NPP2.1 (h) should be amended to include use or disclosure for the purpose of preventing or detecting identity fraud;[251]
- the exception for use or disclosure 'required or authorised' by law should be restricted to 'where expressly or impliedly required by a law'; and[252]
- the definition of 'sensitive information' is problematic and should be deleted.[253]

248 APF, *Submission 32*, p. 13; see also Privacy Act, section 16E.

249 APF, *Submission 32*, p. 7; see also OPC review, pp 88-89.

250 APF, *Submission 32*, p. 15.

251 Baycorp Advantage, *Submission 43*, p. 12; see also Mr Andrew Want, Baycorp Advantage, *Committee Hansard*, 19 May 2005, p. 6.

252 APF, *Submission 32*, p. 20.

253 APF, *Submission 32*, p. 17.