The Senate

Legal and Constitutional References Committee

The real Big Brother: Inquiry into the Privacy Act 1988

June 2005

ISBN 0 642 71498 3

This document was printed by the Senate Printing Unit, Department of the Senate,
Parliament House, Canberra

MEMBERS OF THE REFERENCES COMMITTEE

Members

Senator the Hon Nick Bolkus (Chair), ALP, SA
Senator Marise Payne (Deputy Chair), LP, NSW
Senator Geoff Buckland, ALP, SA
Senator Brian Greig, AD, WA
Senator Linda Kirk, ALP, SA
Senator Nigel Scullion, CLP, NT

Substitute Members

Senator Ridgeway to replace Senator Greig for matters relating to the Indigenous Affairs portfolio
Senator Stott Despoja to replace Senator Greig for the committee's inquiry into the effectiveness and appropriateness of the *Privacy Act 1988*
Senator Mason to replace Senator Scullion for the committee's inquiry into the effectiveness and appropriateness of the *Privacy Act 1988*

Participating Members

Senator the Hon Eric Abetz, LP, TAS
Senator G. Barnett, LP, TAS
Senator A. Bartlett, AD, Qld (for DIMIA)
Senator Mark Bishop, ALP, WA
Senator George Brandis, LP, Qld
Senator Bob Brown, AG, TAS
Senator George Campbell, ALP, NSW
Senator Kim Carr, ALP, VIC
Senator Grant Chapman, LP, SA
Senator the Hon R. Colbeck, LP, TAS
Senator Stephen Conroy, ALP, VIC
Senator Trish Crossin, ALP, NT
Senator Alan Eggleston, LP, WA
Senator Chris Evans, ALP, WA
Senator the Hon John Faulkner, ALP, NSW
Senator Alan Ferguson, LP, SA
Senator Jeannie Ferris, LP, SA
Senator Brian Harradine, Ind, Tas
Senator Gary Humphries, LP, ACT
Senator Susan Knowles, LP, WA
Senator Ross Lightfoot, LP, WA
Senator Joseph Ludwig, ALP, Qld
Senator Sue Mackay, ALP, Tas
Senator Brett Mason, LP, Qld
Senator Julian McGauran, NATS, VIC
Senator Andrew Murray, AD, WA
Senator Kerry Nettle, AG, NSW
Senator Robert Ray, ALP, VIC
Senator the Hon Nick Sherry, ALP, Tas
Senator Ursula Stephens, ALP, NSW
Senator Natasha Stott Despoja, AD, SA
Senator Tsebin Tchen, LP, Vic
Senator John Watson, LP, Tas

Secretariat

Mr Owen Walsh	Secretary
Ms Julie Dennett	Principal Research Officer
Ms Sophie Power	Principal Research Officer
Ms Kelly Paxman	Principal Research Officer
Mr Morgan Pyner	Research Officer (to February 2005)
Ms Marina Seminara	Executive Assistant
Ms Judith Wuest	Executive Assistant (from 2 May – 17 June 2005)

Suite S1.61 Telephone: (02) 6277 3560 Fax: (02) 6277 5794
Parliament House E-mail: legcon.sen@aph.gov.au

TABLE OF CONTENTS

ABBREVIATIONS

ABA	Australian Broadcasting Authority
ABS	Australian Bureau of Statistics
ACA	Australian Consumers' Association
ACCI	Australian Chamber of Commerce and Industry
the Act	*Privacy Act 1988*
ADMA	Australian Direct Marketing Association
AEEMA	Australian Electrical and Electronic Manufacturers' Association
AFP	Australian Federal Police
AIHW	Australian Institute of Health and Welfare
AHEC	Australian Health Ethics Committee
ALRC	Australian Law Reform Commission
AMA	Australian Medical Association
APC	Australian Press Council
APEC	Asia-Pacific Economic Cooperation
APF	Australian Privacy Foundation
ARC	Australian Red Cross
CLAN	Care Leavers of Australia Network
the Code	National Health Privacy Code
CUSCAL	Credit Union Services Corporation (Australia) Limited
DIMIA	Department of Immigration and Multicultural and Indigenous Affairs
DFAT	Department of Foreign Affairs and Trade
EFA	Electronic Frontiers Australia

Essentially Yours report	ALRC and NHMRC, *Essentially Yours: Protection of Human Genetic Information in Australia,* ALRC Report No. 96, March 2003
EU	European Union
EU Data Protection Directive	*Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data*
FIA	Fundraising Institute Australia
HRECs	Human Research Ethics Committees
ICAO	International Civil Aviation Organisation
ICCPR	*International Covenant on Civil and Political Rights*
ID	identification
IFSA	Investment and Financial Services Association
IP address	Internet protocol address
IPPs	Information Privacy Principles
LIV	Law Institute of Victoria
NHMRC	National Health and Medical Research Council
NHPPs	National Health Privacy Principles
NPPs	National Privacy Principles
OECD	Organisation for Economic Cooperation and Development
OECD guidelines	Organisation for Economic Cooperation and Development, *Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data*, 1980
OFPC	Office of the Federal Privacy Commissioner
OPC	Office of the Privacy Commissioner
OPC review	Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988*, March 2005

Passports Act	*Australian Passports Act 2005*
Privacy Act	*Privacy Act 1988*
PSD	public source data company
PIDs	Public Interest Determinations
QIMR	Queensland Institute of Medical Research
RFID	Radio Frequency Identification
Telecommunications Act	*Telecommunications Act 1997*
TFN	Tax File Number
UK	United Kingdom
US	United States
US FDA	United States Food and Drug Administration

CHAPTER 1

INTRODUCTION

Reference

1.1 On 9 December 2004, the Senate agreed to a motion moved by the Australian Democrats and referred the following matters to the Legal and Constitutional References Committee, for inquiry and report by 30 June 2005:

> (a) the overall effectiveness and appropriateness of the *Privacy Act 1988* as a means by which to protect the privacy of Australians, with particular reference to:
>
> (i) international comparisons,
>
> (ii) the capacity of the current legislative regime to respond to new and emerging technologies which have implications for privacy, including:
>
> (A) 'Smart Card' technology and the potential for this to be used to establish a national identification regime,
>
> (B) biometric imaging data,
>
> (C) genetic testing and the potential disclosure and discriminatory use of such information, and
>
> (D) microchips which can be implanted in human beings (for example, as recently authorised by the United States Food and Drug Administration), and
>
> (iii) any legislative changes that may help to provide more comprehensive protection or improve the current regime in any way;
>
> (b) the effectiveness of the *Privacy Amendment (Private Sector) Act 2000* in extending the privacy scheme to the private sector, and any changes which may enhance its effectiveness; and
>
> (c) the resourcing of the Office of the Federal Privacy Commissioner[1] and whether current levels of funding and the powers available to the Federal Privacy Commissioner enable her to properly fulfil her mandate.[2]

---

1 Note that although the terms of reference refer to the Office of the Federal Privacy Commissioner, the office is now referred to as the Office of the Privacy Commissioner. Similarly, the Federal Privacy Commissioner is now known as the Privacy Commissioner. This report uses the title the Office of the Privacy Commissioner and Privacy Commissioner, but it is noted that some submissions, quoted in the report, refer to the Office of the Federal Privacy Commissioner and the Federal Privacy Commissioner.

2 *Journals of the Senate,* No. 11, 9 December 2004, p. 286.

Conduct of the inquiry

1.2 The committee advertised the inquiry in *The Australian* newspaper on 15 December 2004, 2 February 2005, 16 February 2005, 2 March 2005 and 16 March 2005 and wrote to over 90 organisations and individuals, inviting submissions by 25 February 2005. Details of the inquiry were placed on the committee's website.

1.3 The committee received nearly 50 submissions from various individuals and organisations, as well as several supplementary submissions, and these are listed at Appendix 1. Submissions were placed on the committee's website.

1.4 The committee held public hearings in Melbourne on 22 April 2005; in Sydney on 19 May 2005; and in Canberra on 20 May 2005. A list of witnesses who appeared at the hearings is at Appendix 2, and copies of the Hansard transcript are available through the Internet at http://www.aph.gov.au/hansard.

Acknowledgements

1.5 The committee thanks those organisations and individuals who made submissions and gave evidence at public hearings. The committee particularly acknowledges the work of the Australian Law Reform Commission (ALRC) and the Australian Health Ethics Committee (AHEC) of the National Health and Medical Research Council (NHMRC) in their comprehensive report on the protection of human genetic information in Australia.[3] Further, the committee thanks the Office of the Privacy Commissioner (OPC) for its assistance during this inquiry. The OPC's recent report on its review of the private sector provisions (OPC review) was also of great assistance to the committee's inquiry.[4]

Scope of the report

1.6 Chapter 2 provides a background and overview of privacy and the *Privacy Act 1988* (Privacy Act). Chapter 3 considers the capacity of the Privacy Act to deal with emerging technologies, and in particular, those technologies listed in the terms of reference. Chapter 4 examines the effectiveness of the private sector provisions of the Privacy Act, including the recent review of the private sector provisions by the Office of the Privacy Commissioner.

1.7 Chapter 5 considers a range of other issues raised during the committee's inquiry relating to the overall effectiveness and appropriateness of the Privacy Act. Chapter 6 looks at the resourcing and powers of the Office of the Privacy

---

3 ALRC and NHMRC, *Essentially Yours: Protection of Human Genetic Information in Australia,* ALRC 96, 2003, available at: http://www.austlii.edu.au/au/other/alrc/publications/reports/96/

4 Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988*, March 2005 (OPC review), available at: http://www.privacy.gov.au/act/review/index.html

Commissioner. Issues relating to privacy and international comparisons, as listed in term of reference (a)(i) are considered through the report. Finally, chapter 7 presents a summary of the Committee's conclusions and its recommendations on a range of matters relating to the Privacy Act.

Note on references

1.8 References in this report are to individual submissions as received by the committee, not to a bound volume. References to the Committee Hansard are to the proof Hansard: page numbers may vary between the proof and the official Hansard transcript.

CHAPTER 2

BACKGROUND

2.1 This chapter provides some background to the Privacy Act, including:

- concepts of privacy;
- privacy under international and common law;
- history of the Privacy Act;
- key provisions of the Privacy Act; and
- community attitudes towards privacy.

Concepts of privacy

2.2 As the Law Reform Commission (as it was then known) noted in its 1983 report on privacy, 'the very term 'privacy' is one fraught with difficulty. The concept is an elusive one.'[1] Privacy is often referred to as the 'right to be let alone'.[2] Professor Zelman Cowen, in the 1969 Boyer lectures, observed that:

> A man without privacy is a man without dignity; the fear that Big Brother is watching and listening threatens the freedom of the individual no less than the prison bars.[3]

2.3 Similarly, Mr Bill O'Shea of the Law Institute of Victoria (LIV) remarked during this inquiry that 'an individual's privacy is fundamental to their human dignity'.[4] Mr Paul Chadwick, the Victorian Privacy Commissioner, addressed the committee on the purpose of privacy:

> Firstly, it [privacy] is understood to be essential to selfhood—to the creation of the self. It is as fundamental as that, and it is why humans retreat to solitude at times or keep their reserve in the company of others. Secondly, it is understood to be fundamental to the creation and maintenance of intimacy between humans. Unless the privacy of your relationship with your nearest and dearest is observed by the partners, trust

---

1 The Law Reform Commission, *Privacy*, ALRC Report No. 22, Volume 1, 1983, p. 10.

2 Samuel Warren and Louis Brandeis, 1890, 'The Right to Privacy', 4 *Harvard Law Review* 193; see also Malcolm Crompton, former Federal Privacy Commissioner, "Proof of ID Required? Getting Identity Management Right", *Speech to the Australian IT Security Forum*, 30 March 2004, p. 2, http://www.privacy.gov.au/news/speeches/sp1_04p.pdf (accessed 24 May 2005).

3 Zelman Cowen, 1969, "The Private Man", The Boyer Lectures, Australian Broadcasting Commission, pp 9-10 from Malcolm Crompton, former Federal Privacy Commissioner, "Proof of ID Required? Getting Identity Management Right", *Speech to the Australian IT Security Forum*, 30 March 2004, p. 2, http://www.privacy.gov.au/news/speeches/sp1_04p.pdf (accessed 24 May 2005).

4 *Committee Hansard*, 22 April 2005, p. 14.

> is lost. So privacy as essential to intimacy is the second purpose of privacy among humans. Thirdly, not to be downplayed but also not to be overplayed, is privacy as liberty.[5]

2.4 'Privacy' is often broken down into different elements. Mr Chadwick discussed five dimensions of privacy as including: privacy of the body; privacy of the home; privacy from surveillance; privacy from eavesdropping; and information privacy.[6] However, the Privacy Commissioner, Ms Karen Curtis, pointed out to the committee in Sydney that:

> …while our Privacy Act is about the protection of personal information or sensitive information, it is really about data protection. It is not about privacy in the broader sense of bodily privacy or privacy in other areas. I think 'privacy' is often seen as a catch-all, and so our Privacy Act does not address all aspects of territorial privacy or bodily privacy. The Privacy Act addresses the collection, use, disclosure and storage of personal information held by Commonwealth government departments and agencies, ACT government departments and agencies and also the private sector across Australia.[7]

2.5 Despite this, the Australian Privacy Foundation (APF) urged this inquiry:

> …to consider what additional protection needs to be put in place to deal with contemporary threats, going beyond information privacy principles to limit the development of a surveillance society and protect individuals from assaults on their physical integrity such as mandatory drug and DNA testing and increasingly prevalent and intrusive searches, and from other intrusions (such as by telemarketing or media harassment). These forms of privacy invasion may not involve the creation of a record of personal information, and yet are just as important in terms of a more general "right to be let alone".[8]

2.6 Mr Paul Chadwick argued the significance of privacy is growing, for three key reasons.[9] The first reason was technological developments; the second related to international obligations and developments. Finally, Mr Chadwick argued that we are going through a 'recalibration of liberty and security':[10]

> The third factor that explains why the Privacy Act is growing in significance is 11 September 2001 and what has flowed from that in terms of public policy. We are now recalibrating the balance between liberty and security. Privacy is legitimately a subset of liberty, and those of you who

---

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

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

7 *Committee Hansard*, 19 May 2005, p. 51.

8 *Submission 32*, p. 6.

9 *Committee Hansard*, 22 April 2005, p. 4; see also *Submission 33*, p. 2.

10 *Committee Hansard*, 22 April 2005, p. 10.

> have had to address things like the ASIO [Australian Security Intelligence Organisation] legislation et cetera will be aware of those arguments.[11]

2.7 Similarly, Mr Andrew Want of Baycorp Advantage suggested that, among other things, one of the emerging challenges in the area of privacy:

> …is the balance between identity management and anonymity in the context of terrorism and security. There is an obvious societal push for greater security following September 11. The risk is that the pendulum might swing too far and individual privacy might be lost in the mix. There needs to be a serious debate about what the benefit for society is and what the policy objective of privacy regulation is in this new context. So it is not just about economic efficiency; it is also about the balance of individual liberty in the face of the challenges society is now dealing with out of the remnants of September 11.[12]

2.8 However, Ms Anna Johnston of the APF raised concerns about the impact of recent events on the Privacy Act, and especially:

> …the extent to which the so-called war on terror is used to justify an abandonment of any rationality in our policy process, such that new proposals are not calmly weighed in terms of necessity, proportionality or reasonableness, effectiveness and looking at alternative options.[13]

2.9 In particular, Ms Johnston strongly expressed the view that:

> …we reject the notion that we are somehow living in a new age of terror, justifying the abandonment of long-cherished values or hard-won liberties…
>
> ...post September 11, we do not believe the world actually changed that much. Even more so, we utterly reject any suggestion that privacy or indeed other human rights somehow stand in the way of security or good government. Privacy ensures the freedom of speech and freedom of association necessary for stable and democratic government. Furthermore, privacy, like openness, transparency and freedom of information, is about ensuring the accountability of government and business. In doing so, respect for privacy and the robust enforcement of privacy principles and privacy rights can only strengthen the fair and expose the corrupt.[14]

2.10 Similarly, Mr Bill O'Shea from the LIV observed:

> The default position should be that we protect people's privacy and that you as legislators do the same...if we have a drift in this community based on 9/11 or the US alliance or whatever else we are concerned about the drift

---

11 *Committee Hansard*, 22 April 2005, p. 4.

12 Mr Andrew Want, *Committee Hansard*, 19 May 2005, p. 2.

13 *Committee Hansard*, 19 May 2005, p. 12.

14 *Committee Hansard*, 19 May 2005, pp 12-13.

> will inexorably be to take away people's dignity and progressively take away more rights by privacy infringement creep.[15]

2.11 As Mr Timothy Pilgrim of the OPC remarked:

> …it is the issue of the balance. We would say that in certain circumstances privacy cannot be an absolute. There has to be that balance achieved between the needs of the individual and the broader community.[16]

Privacy protection under international and other Australian law

International law

2.12 There are several key sources of international law and standards relevant to privacy protection in Australia.[17] In particular, the *International Covenant on Civil and Political Rights* (ICCPR) recognises the right to privacy in Article 17. It states:

> (1) No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation.
>
> (2) Everyone has the right to the protection of the law against such interference or attacks.

2.13 Article 12 of the *Universal Declaration of Human Rights* contains an almost identical provision.

2.14 The Organisation for Economic Cooperation and Development's (OECD) *Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data* (OECD guidelines) were adopted in 1980. The guidelines set out eight `Basic Principles of National Application' (guidelines 7 to 14) to be followed by OECD countries. The guidelines set out the way personal information about individuals should be collected, stored, used and disclosed – consistent with the above mentioned international laws. They also set out mechanisms by which individuals can gain access to, and have amended, information about them held by others.[18]

2.15 According to the OPC, the Privacy Act gives effect to Article 17 of the ICCPR and the OECD Guidelines. In particular, the OECD guidelines provided the basis for the Information Privacy Principles contained in the Privacy Act.[19] The

---

15 *Committee Hansard*, 22 April 2005, p. 17.

16 *Committee Hansard*, 19 May 2005, p. 51.

17 See further Senate Legal and Constitutional References Committee, *Privacy and the Private Sector: Inquiry into Privacy Issues, including the Privacy Amendment Bill 1998*, March 1999, pp 42-51.

18 OPC, *The Operation of the Privacy Act Annual Report: 1 July 2003 – 30 June 2004*, p. 84. The OECD guidelines are available at: www.oecd.org.

19 OPC review, p. 46.

Preamble to the Privacy Act also specifically refers to the ICCPR and the OECD Guidelines:

> WHEREAS Australia is a party to the International Covenant on Civil and Political Rights, the English text of which is set out in Schedule 2 to the Human Rights and Equal Opportunity Commission Act 1986:
>
> AND WHEREAS, by that Covenant, Australia has undertaken to adopt such legislative measures as may be necessary to give effect to the right of persons not to be subjected to arbitrary or unlawful interference with their privacy, family, home or correspondence:
>
> AND WHEREAS Australia is a member of the Organisation for Economic Co-operation and Development:
>
> AND WHEREAS the Council of that Organisation has recommended that member countries take into account in their domestic legislation the principles concerning the protection of privacy and individual liberties set forth in Guidelines annexed to the recommendation:
>
> AND WHEREAS Australia has informed that Organisation that it will participate in the recommendation concerning those Guidelines…

2.16 The European Union's (EU) *Directive on the protection of individuals with regard to the processing of personal data and on the free movement of such data* (EU Data Protection Directive)[20] is also relevant to Australia privacy law. In particular, the EU Data Protection Directive contains provisions to ensure that European individuals do not lose privacy protection rights when information about them is transferred to other jurisdictions outside the EU. If the laws of the destination country do not provide 'adequate' data protection standards, as determined by the EU, then there are restrictions on the transfer of information to that other jurisdiction.[21]

2.17 Indeed, one of the stated purposes of the *Privacy Amendment (Private Sector) Act 2000* was to facilitate trade with EU members.[22] However, to date, the EU has not recognised Australia's privacy laws as "adequate" for the purposes of the EU Data Protection Directive. Only a few countries, such as Canada, Switzerland, and the United States have been recognised in this manner.[23] Indeed, the issue of whether the Privacy Act meets the EU directive requirements, and the extent to which this has had any impact on trade with the EU, were issues raised in submissions and evidence to this inquiry. This issue is considered later in this report.

---

20 Directive 95/46/EC.

21 See especially articles 25 and 26. See further Nigel Waters, 'The European influence on privacy law and practice', *Privacy Law and Policy Report*, Vol. 9, No. 8, 2003, pp 150-155; Peter Ford, 'Implementing the EC Directive on Data Protection – an outside perspective' *Privacy Law and Policy Report*, Vol. 9, No. 8, 2003, pp 141-149.

22 Attorney-General, the Hon. Daryl Williams AM QC MP, Second Reading Speech, *Privacy Amendment (Private Sector) Bill 2000*, Hansard, 12 April 2000, p. 15749.

23 See further http://europa.eu.int/comm/internal_market/privacy/adequacy_en.htm (accessed 9 February 2005).

2.18 Another recent international development is the endorsement in November 2004 by Asia-Pacific Economic Cooperation (APEC) Ministers of the APEC Privacy Framework. Again, this is discussed further later in this report.

Other Australian law

2.19 The Australian Constitution does not expressly protect privacy nor does it contain a specific head of Commonwealth legislative power on which to base legislative protection.[24] As Mr O'Shea of the LIV observed, there is no right to privacy under the Australian Constitution.[25] Several submitters expressed support for consideration of the incorporation of a right to privacy in the Constitution, or a Bill of Rights.[26]

2.20 Until recently, there was also no general right of privacy at common law in Australia. However, in 2003, the District Court of Queensland recognised a tort of invasion of privacy in the case of *Grosse v Purvis*.[27] This case followed the High Court case of *Lenah Game Meats*, in which the High Court arguably left open the possibility of a tort of invasion of privacy.[28]

2.21 It is also noted that a number of State and Territory jurisdictions have also enacted their own privacy legislation.[29]

History of the Privacy Act

2.22 The Privacy Act was enacted in 1988, following the demise of the 'Australia Card' proposal. The Privacy Act was initially directed at the protection of personal information held by Commonwealth government departments and agencies, as well as safeguards for the collection and use of tax file numbers. In 1990, the Privacy Act was amended to insert Part IIIA, which regulates credit reporting and information held by credit reporting agencies and credit providers.[30]

---

24 NHMRC, *Submission 20, Attachment D*, p. 1.

25 Mr Bill O'Shea, *Committee Hansard*, 22 April 2005, pp 14, 19.

26 See, for example, Victorian Privacy Commissioner, *Submission 33*, p. 4; and Mr Bill O'Shea, Law Institute of Victoria, *Committee Hansard*, 22 April 2005, pp 14, 19.

27 [2003] QDC 151. See also Greg Heaton, 'Privacy – boldly going where defamation hasn't gone before', *Media & Arts Law Review*, vol. 9 no. 4, pp 295- 316.

28 *ABC v Lenah Game Meats Pty Ltd* (2001) 208 CLR 199. See further Dr Robert Dean, 'A Right to privacy', *Australian Law Journal*, vol. 78, no. 2, pp. 114- 125; Greg Heaton, 'Privacy – boldly going where defamation hasn't gone before', *Media & Arts Law Review*, vol. 9 no. 4, pp. 295- 316; see also Morag Donaldson, 'Do Australians have a legal right to privacy?', *Parliamentary Library Research Note*, 14 March 2005, no. 37 2004-05.

29 See, for example, the table of legislation in NHMRC, *Submission 20, Attachment D*, p. 2.

30 See further OPC, *Federal Privacy Law History*, at http://www.privacy.gov.au/act/history/index.html (accessed 9 February 2005).

2.23 The *Privacy Amendment (Private Sector) Act 2000* commenced in December 2001, with the aim of strengthening privacy protection in the private sector by establishing national standards for the handling of personal information by the private sector. Before this, the private sector was covered by a voluntary system of 'National Principles for the Fair Handling of Personal Information'. Among other things, the *Privacy Amendment (Private Sector) Act 2000* established the 'National Privacy Principles' and provided for approved privacy codes. As noted above, extending privacy protection to the private sector was partly in response to the EU Data Protection Directive. Other aims of the *Privacy Amendment (Private Sector) Act 2000* included: ensuring that Australia business and consumers take full advantage of the opportunities presented by electronic commerce and the information economy; and allaying concerns about the security of personal information when doing business online.[31]

Key provisions of the Privacy Act 1988

2.24 The Privacy Act protects personal information in four key ways:

- The *Information Privacy Principles* (IPPs) in section 14 of the Privacy Act govern the collection, storage, use and disclosure of an individual's personal information. They also provide for individual access to, and correction of, their own personal information. These principles are based on the OECD guidelines and apply to personal information handled by Commonwealth and ACT Government agencies.
- The *National Privacy Principles* (NPPs) in schedule 3 of the Privacy Act regulate the way private sector organisations handle personal information (unless replaced by a code approved by the Commissioner under section 18BB of the Privacy Act). These principles cover the collection, storage, use and disclosure, and access obligations of organisations.
- The Act also prevents individuals' Tax File Numbers (TFNs) from being used as a national identification system and gives individuals the right to withhold this information. Where a TFN is provided, its use is limited to purposes relating to taxation, government assistance or superannuation. Under the Act, the Privacy Commissioner issues and enforces legally binding guidelines.[32]
- Part IIIA of the Privacy Act places safeguards on the handling of individuals' consumer credit information by the credit industry. Unlike other provisions of the Privacy Act, strict penalties apply where these provisions are knowingly breached.[33]

---

31 Attorney-General, the Hon. Daryl Williams AM QC MP, Second Reading Speech, *Privacy Amendment (Private Sector) Bill 2000*, Hansard, 12 April 2000, p. 15749.

32 See especially Privacy Act, ss. 17 and 18.

33 OPC, *The Operation of the Privacy Act Annual Report: 1 July 2003 – 30 June 2004*, pp 84-85.

2.25 A key definition in the Privacy Act is that of 'personal information', which is defined in section 6 to mean:

> information or an opinion (including information or an opinion forming part of a database), whether true or not, and whether recorded in a material form or not, about an individual whose identity is apparent, or can reasonably be ascertained, from the information or opinion.

2.26 Section 6 also defines 'sensitive information' to mean:

> (a) information or an opinion (that is also personal information) about an individual's racial or ethnic origin; political opinions; membership of a political association; religious beliefs or affiliations; philosophical beliefs; membership of a professional or trade association; membership of a trade union; sexual preferences or practices; or criminal record; or
>
> (b) health information about an individual.

2.27 Part IV of the Privacy Act provides for the establishment of the Office of the Privacy Commissioner and the appointment of a Privacy Commissioner. The Privacy Commissioner has several specific powers and functions under the Privacy Act. These include: complaint handling; investigating breaches of the Act; compliance auditing; providing policy advice and promoting community awareness.[34]

2.28 Part VI of the Privacy Act gives the Privacy Commissioner the power to issue 'public interest determinations'. That is, to determine that an act or practice of a Commonwealth or ACT government agency, or a private sector organisation, which may otherwise constitute a breach of an Information Privacy Principle, a National Privacy Principle or an approved privacy code, shall be regarded as not breaching that principle or approved code. The Privacy Commissioner has also released a number of guidelines, both binding and advisory, to assist organisations to comply with the Act.[35]

2.29 The Privacy Act also contains many exemptions and exceptions. For example, the legislation does not apply to:

- certain small businesses (for example, businesses with an annual turnover of less than $3 million and not disclosing personal information for a benefit);[36]
- political acts and practices;[37]
- employee records held by current or former employers;[38] or
- acts and practices of the media in the course of journalism.[39]

---

34 Privacy Act, ss. 27, 28 and 28A.

35 See further: http://www.privacy.gov.au/act/guidelines/index.html.

36 Privacy Act, ss. 6C-6EA.

37 Privacy Act, s. 7C.

38 Privacy Act, s. 7B(3).

Community attitudes towards privacy

2.30 The OPC has commissioned surveys to gauge community attitudes towards privacy, as well as community knowledge of their privacy rights. The most recent survey, conducted in 2004, contained some interesting findings.[40] The survey showed that there appear to be low levels of knowledge about rights to protect privacy:

> Sixty per cent [of respondents] claimed to be aware that Federal privacy laws existed, up from 43% in 2001. By contrast, only 34% of respondents were aware the Federal Privacy Commissioner existed. When asked to whom they would report the misuse of their personal information, 29% said they didn't know.[41]

2.31 In its submission, the Australian Direct Marketing Association (ADMA) noted that it conducted research which also indicated a low level of awareness of the Privacy Act and the Privacy Commissioner.[42]

2.32 However, the survey commissioned by OPC also found that most respondents considered the following hypothetical situations as an invasion of privacy:

> · a business that you don't know gets hold of your personal information (94%);
>
> · a business monitors your activities on the internet, recording information on the sites you visit without your knowledge (93%);
>
> · you supply your information to a business for a specific purpose and the business uses it for another purpose (93%); and
>
> · a business asks for irrelevant personal information that doesn't seem relevant to the purpose of the transaction (94%).[43]

2.33 However, only 16% of respondents considered that being asked to show identification, such as a driver's license or passport, to establish your identity would be an invasion of privacy.[44]

---

39 Privacy Act, s. 7B(4).

40 Roy Morgan Research for the Office of the Federal Privacy Commissioner, *Community Attitudes Towards Privacy*, 18 June 2004, http://www.privacy.gov.au/publications/rcommunity04.pdf (accessed 9 February 2005); see also OPC review, Appendix 6.

41 Ibid, Executive Summary, p. 1.

42 *Submission 38*, p. 8. Other aspects of the ADMA's research are considered in the discussion in relation to direct marketing in Chapter 4 of this report.

43 Roy Morgan Research for the Office of the Federal Privacy Commissioner, *Community Attitudes Towards Privacy*, 18 June 2004, Executive Summary, p. 2, at: http://www.privacy.gov.au/publications/rcommunity04.pdf (accessed 9 February 2005).

44 Roy Morgan Research for the Office of the Federal Privacy Commissioner, *Community Attitudes Towards Privacy*, 18 June 2004, Executive Summary, p. 2, at: http://www.privacy.gov.au/publications/rcommunity04.pdf (accessed 9 February 2005).

2.34 In relation to interactions with government:

> Just over half (53%) of respondents were in favour of being issued with a unique number to be used for identification when accessing all Australian government services, slightly fewer (41%) were against. The majority of respondents agreed governments should be allowed to cross reference or share information, but only in some circumstances (62%) … To prevent or reduce crime (68%) was the scenario under which most respondents felt it was acceptable to cross reference information, followed by the purpose of updating basic information like address details (58%) and to reduce costs, or improve efficiency (51%).[45]

2.35 With health services, 57% of respondents agreed that to enable the government to better track the use of health care services, individuals should have a number assigned to them for use when accessing any health service.[46]

2.36 Further details of the 2004 survey commissioned by the OPC are contained in the OPC's report on the private sector provisions.[47]

---

45 Roy Morgan Research for the Office of the Federal Privacy Commissioner, *Community Attitudes Towards Privacy*, 18 June 2004, Executive Summary, p. 3, at: http://www.privacy.gov.au/publications/rcommunity04.pdf (accessed 9 February 2005).

46 Roy Morgan Research for the Office of the Federal Privacy Commissioner, *Community Attitudes Towards Privacy*, 18 June 2004, Executive Summary, p. 3, at: http://www.privacy.gov.au/publications/rcommunity04.pdf (accessed 9 February 2005).

47 OPC review, Appendix 6.

CHAPTER 3

EMERGING TECHNOLOGIES

3.1 This chapter will consider issues raised in submissions and evidence in relation to the capacity of the Privacy Act to respond to new and emerging technologies, including:

- the capacity of the Privacy Act to respond to new technologies in general;
- smartcards and national identification (ID) schemes;
- biometric data, including proposed biometric passports;
- genetic testing and discrimination;
- microchip implants and radio frequency identification (RFID) technology; and
- other technologies and related issues.

3.2 Term of reference (a)(ii) specifically singles out four particular technologies: smartcards; biometric imaging data; genetic testing; and human microchip implants. Several submissions suggested that the same privacy principles arise in relation to all these technologies.[1] The committee notes that there is also some overlap between these technologies. For example, smartcards and microchips may contain genetic and biometric information. In addition, genetic information is a type of biometric data.[2] However, this chapter will first consider the capacity of the Privacy Act to respond to new technologies in general.

In general

3.3 Many submissions argued that the Privacy Act is not keeping pace with the challenges of developing technology.[3] Some suggested that the Privacy Act needs to be updated to reflect new technological developments.[4] Others suggested that a complete overhaul of privacy legislation is required.[5] For example, Ms Irene Graham from Electronic Frontiers Australia (EFA) expressed the view that:

> …the current legislative regime does not adequately protect the privacy of Australians in relation to technologies that have been in use for a decade, so

---

1 See, for example, Caroline Chisholm Centre for Health Ethics, *Submission 21*, p. 6; LIV, *Submission 37*, pp 5-6.

2 ALRC, *Submission* 18, p. 7.

3 See, for example, Australian Consumers' Association, *Submission 15*, p. 1; APF, *Submission 32*, pp 10-11; LIV, *Submission 37*, p. 5; Mr Roger Clarke, *Submission 28*, p. 2; EFA, *Submission 17*, p. 7.

4 See, for example, Centre for Law and Genetics, *Submission 24*, pp 3-4.

5 See, for example, Mr Roger Clarke, *Submission 28*, pp 2, 4.

> we certainly do not believe that it has the capacity to respond adequately to new and emerging technologies.[6]

3.4 Mr Roger Clarke argued that the Privacy Act is 'utterly inadequate' to protect the privacy of Australians. Mr Clarke discussed the origins of the Privacy Act, noting its implementation of the 1980 OECD guidelines, and suggested that:

> Because of its origins, the Act addressed technology of a past era, the 1970s. There has been no substantive review, and there have been no substantive enhancements, since that time. Meanwhile, it has been subject to continual weakening…[7]

3.5 Similarly, Mr Bill O'Shea from the LIV argued that the Privacy Act:

> …is falling behind new technologies and needs to catch up, particularly with smart cards, genetic information and biometric encryption. It is clear, and I do not think I need to elaborate, that the [A]ct needs to catch up on that.[8]

3.6 In the same vein, Ms Anna Johnston of the APF argued that one of the main challenges to the Privacy Act is 'the rapid pace of technological change':

> …the Privacy Act alone and in its current state is not enough to protect the privacy of Australians…the Privacy Act is almost 20 years old and deserving of review to ensure its robustness and appropriateness to meet new challenges.[9]

3.7 Similarly, the Australian Consumers' Association (ACA) were concerned that:

> …the Privacy Act has not set a framework to keep pace with developing technological challenges. Other 'instruments', specific Federal legislation like the Spam Act and industry codes like the ACIF [Australian Communications Industry Forum] SMS code and the ADMA m-commerce code, have been required to advance consumer protection beyond the provisions and outside the framework of the Privacy Act in areas with considerable privacy implications.[10]

3.8 In particular, Mr Charles Britton of the ACA observed that:

> …both government and industry have had to act outside the framework to the Privacy Act in areas like spam and there are gaps opening up in areas like surveillance, biometrics and radiofrequency identification.[11]

---

6 *Committee Hansard*, 22 April 2005, p. 41; see also *Submission 17*, p. 7.

7 *Submission 28*, p. 1.

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

9 *Committee Hansard*, 19 May 2005, p. 12.

10 *Submission 15*, p. 1.

11 *Committee Hansard*, 19 May 2005, p. 22.

3.9 The Centre for Law and Genetics noted the words of Justice Michael Kirby that:

> [t]here has been little endeavour to reflect the major scientific and technological developments of the last fifty years, and their impact on human rights, in a conceptual way. Instead, old human rights instruments developed for earlier times are scrutinised for their possible utility in solving controversies presented by the new technology. Piece-meal legislation is enacted. No Luther of jurisprudence has emerged to pull together the implications of nuclear physics, informatics and biotechnology for twenty first century man or woman.[12]

Technological neutrality

3.10 On the other hand, some submitters believed that the Privacy Act does not need to be amended to deal with the introduction of new technologies, or supported the notion that the privacy legislation should remain 'technology neutral'.[13] Indeed, the explanatory memorandum to the Privacy Amendment (Private Sector) Bill 2000 stated:

> The speed at which electronic commerce is evolving and changing makes it difficult for existing laws to be adapted. Any arrangements that are put in place need to provide an adequate and enforceable level of security and protection of personal information, while being flexible and technology-neutral so they can adjust to changing circumstances and emerging technologies.[14]

3.11 The APF supported this approach:

> …it is essential that any legislative privacy protection regime is as 'technology neutral' as possible, as we simply cannot predict the next innovations or their implications.[15]

3.12 Baycorp Advantage also agreed that 'privacy regulation should continue to seek technological neutrality as an objective.' However, Baycorp Advantage further argued that:

> The privacy impact of new technologies and technological practices should be constantly assessed, but any regulatory measure that seeks to impede developing technology or practice should meet a very stringent test

---

12 Michael Kirby, 'Privacy in Cyberspace' (1998) 21 *University of New South Wales Law Journal* 323; see also *Submission 24*, p. 3.

13 See, for example, Sony, *Submission 14*, pp 1-2; FIA, *Submission 3*, p. 3; ANZ, *Submission 6*, p. 5; APF, *Submission 32*, p. 10; Baycorp Advantage, *Submission 43*, p. 11; ADMA, *Submission* 38, pp 3 and 6; see also Senate Select Committee on Information Technologies, *Cookie Monsters? Privacy in the Information Society*, November 2000, pp 57-61.

14 Privacy Amendment (Private Sector) Bill 2000, *Revised Explanatory Memorandum*, p. 10.

15 *Submission 32*, p. 10.

> establishing both serious harm and the absence of any alternative, non-regulatory response.[16]

3.13 Mr Charles Britton of the ACA similarly felt that 'technological neutrality is a very useful policy and legislative and regulatory tool.' However, he also warned that:

> People sometimes confuse technological neutrality with some sort of static thing that then does not change. It is always going to be challenged and the challenges will be specific. I think there is always the temptation to become specific in the response and I think that is a mistake. It is harder work, but we need to work through what those challenges are and then come up with the technologically neutral response.[17]

3.14 In contrast, Mr Roger Clarke raised strong objections to the notion of 'technology neutrality':

> The Attorney-General's Department has adopted the mantra of 'technology neutrality' as an excuse for avoiding any need to confront the ravages wrought on laws by changes in technology. The notion of technology neutrality is intuitively appealing; but in many circumstances it fails. For example, there was no need to create laws relating to nuclear proliferation until nuclear technology came along. Similarly, constraints on aircraft breaking the sound barrier over settled areas were unnecessary while such speeds were theoretical. Moreover, regulation of such technologies was simply inconceivable until the technologies were invented. It was therefore sheer fluke if any form of regulatory constraint existed when they were first deployed.[18]

3.15 Indeed, some submissions suggested that other, more prescriptive rules or principles are required to deal with new technologies. For example, the LIV argued that:

> …there are ways in which some new and emerging technologies are being applied to processes, services and products that represent a significantly high risk to privacy so much so that it is not sufficient to rely solely on the broad principles in the Privacy Act. The LIV recommends that more prescriptive, specific, rules are required.[19]

3.16 The LIV then gave the following examples:

> An early example is the Data Matching Program (Assistance and Tax) Act 1980 (Cth), which contains detailed provisions to regulate the computer matching of personal information using Tax File Numbers. A more recent example is the Spam Act 2003 (Cth) which addresses directly the emergence of commercial electronic messages. These statutes reinforce and

---

16 *Submission 43*, p. 11.

17 *Committee Hansard*, 19 May 2005, p. 24.

18 *Submission 28*, p. 2.

19 *Submission 37*, p. 9.

> build on the essential principles set out in the Privacy Act in relation to the collection, storage, use, disclosure, accessibility and destruction of personal information.[20]

3.17 However, as discussed above, others argued that the need for legislation such as the *Spam Act 2003* was because the Privacy Act had failed to meet the challenges posed by new technologies. Further, as will be discussed in chapter 4 of this report, other submissions were concerned that the introduction of legislation to address specific technologies can also create inconsistency.[21]

Definition of 'personal information'

3.18 Several submissions suggested that the definition of 'personal information' in section 6 of the Privacy Act needs to be improved and updated to deal with new technologies and new methods of collecting information.[22]

3.19 For example, the APF suggested that the definition should be extended to include information that enables an individual not only to be identified, but also contacted.[23] Further, Ms Anna Johnston observed:

> …the definition in the federal Privacy Act only incorporates information that has been recorded. There is some ambiguity around whether photographs and images are included. By contrast, the New South Wales privacy legislation, for example, quite clearly includes information that has not yet been recorded in a material form. To give an example, the use of live CCTV, where it is not recorded but someone is using surveillance in a live format, is clearly covered by state legislation but not by the federal legislation.[24]

3.20 Similarly, EFA felt that the definition was inadequate in the context of the electronic environment, and that it should be:

> …extended to cover identifiers irrespective of whether it is obvious to the collector or discloser that an individual's identity can reasonably be

---

20 *Submission 37*, p. 9.

21 See, for example, Fundraising Institute Australia (FIA), *Submission 3*, p. 4; ADMA, *Submission 28,* p. 7.

22 See, for example, Centre for Law and Genetics, *Submission 24*, p. 3; EFA, *Submission 17*, pp 32-33; APF, *Submission 32*, p. 7. Note that it was also suggested that the definitions of 'health information' and 'sensitive information' should be amended expressly to include human genetic information. This will be discussed further later in this chapter. See also see also Senate Select Committee on Information Technologies, *Cookie Monsters? Privacy in the Information Society*, November 2000, pp 61-65.

23 *Submission 32*, p. 7; see also Dr Anthony Place, *Submission 22*, p. 2.

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

ascertained from that identifier and whether or not an individual can be contacted by use of that identifier.[25]

3.21 Ms Irene Graham from EFA explained:

> With new technologies, particularly in the area of telecommunications—it is already occurring in relation to biometrics and so forth—there are a huge number of questions about what the definition of 'personal information' actually means. It refers to information from which a person's identity can be reasonably ascertained. Over the years to date it has been generally accepted that information like a street address or a person's telephone number is arguably personal information because you can identify individuals from their street address or their phone number. Now, particularly in the internet space, we have a situation where individuals using their laptops or their computers at home are having IP addresses allocated to their computers. Some people will argue that an IP address is not personal information because it identifies a computer. But in our view it is exactly the same as a phone number or a street address.[26]

3.22 EFA suggested that the definition should be extended to cover:

> …any information which enables interactions with an individual on a personalised basis, or enables tracking or monitoring of an individual's activities and/or communication patterns, or enables an individual to be contacted.[27]

3.23 In support of this argument, EFA pointed to overseas research indicating that computer IP addresses are considered to be personal data in some overseas jurisdictions.[28] EFA also asserted that Australia should take a lead in endeavours to protect the privacy of Internet users, 'as it did for example in enacting the *Spam Act 2003*.'[29]

3.24 In contrast, others believed that the definition of personal information should remain focussed on the ability to identify individuals, rather than extending the provisions to include the ability to contact individuals.[30] In particular, Hitwise[31] believed that changing the definition of personal information in this way would have 'significant implications for the Internet industry and e-commerce, as it would impact

---

25 *Submission 17*, p. 32.

26 *Committee Hansard*, 22 April 2005, pp 41-42; see also EFA, *Submission 17A*, pp 3-4.

27 *Submission 17*, p. 33.

28 *Submission 17A*, p. 5.

29 *Submission 17A*, p. 5.

30 See, for example, ADMA, *Submission* 38, p. 5; Hitwise, *Submission 47*, p. 4.

31 Hitwise is a company which provides a website-usage analysis service: see Hitwise, *Submission 47*.

upon how every business with an online presence conducts its business.'[32] Hitwise also maintained that EFA had not put forward any sound policy reasons as to why Australia should extend the definition of personal information.[33]

Privacy impact assessments

3.25 Another suggestion put forward in submissions was that privacy impact assessments should be conducted prior to the implementation of new technologies.[34] The APF submitted that privacy impact assessments are:

> …now a mandatory requirement in several jurisdictions including the USA and Canada. Criteria should be developed, drawing on international experience, for triggering such a requirement under the Privacy Act. PIAs [Privacy Impact Assessments] should be conducted by independent assessors but paid for by scheme proponents, with the Privacy Commissioner setting and monitoring appropriate standards.[35]

3.26 Similarly, the LIV suggested that government agencies and organisations should be required to prepare a privacy impact assessment:

> …if they propose to apply new technologies in a way that entails collecting more information than before, sharing it more freely than before, using existing or new information for new purposes not envisaged before, or holding it longer than before. If the Privacy Impact Assessment reveals significant risks in the view of the Privacy Commissioner, further regulation could be required, whether it be a code, regulations or new legislation. [36]

3.27 The LIV continued:

> We suggest that Privacy Impact Assessments will introduce a process under which due consideration should be given to the privacy rights of individuals in the context of other public interests, such as national security, law enforcement and administrative efficiency. Without a predictable, structured process to assess the privacy implications of proposals that could have a broad and significant impact on the community, each new idea is likely to attract controversy and criticism until the necessary analysis has been done.[37]

---

32 *Submission 47*, p. 4 cf EFA, *Submission 17A*, pp 7-8.

33 *Submission 47*, p. 4.

34 See, for example, Office of the Victorian Privacy Commissioner, *Submission 33*, p. 5; LIV, *Submission 37*, p. 5; APF, *Submission 32*, p. 11.

35 *Submission 32*, p. 11.

36 *Submission 37*, pp 6-7.

37 *Submission 37*, p. 7.

3.28 Mr Bill O'Shea from the LIV elaborated on this during the Committee's hearing in Melbourne, suggesting that there are various ways such privacy impact assessments could be done:

> For example, if Medibank Private or Medicare were to change the way they collect information on behalf of members we would expect that an impact statement as to what that change would be would be provided to all members. If that were to go through parliament we would expect that impact statement to be part of the legislation, certainly either incorporated in the second reading speech or made available to the public.
>
> …If there were other examples where legislation was not required, we would expect the peak body for the organisation that had that information to provide a privacy impact assessment for those people in the public who were dealing with it. If, for example, it involved the Insurance Council of Australia we would expect to be required to produce for the public a privacy impact assessment of whatever they were planning to do.[38]

3.29 Ms Irene Graham from EFA expressed qualified support for the concept of privacy impact assessments, but cautioned that if the OPC were to conduct the assessments, funding and resourcing issues would need to be addressed.[39]

3.30 The OPC acknowledged that it encouraged the use of privacy impact assessments:

> We have advised that [government] departments should consider a privacy impact assessment process whereby they examine any new policy proposal in the light of the impacts on a person's privacy, and that, each step along the way, they should continuously look to see what it is they are proposing to do and whether it is the best way. Things can be done in a privacy-enhancing way rather than in a privacy-intrusive way. As we often say, the biggest invasion of a person's privacy is that their identity is stolen, so we need to address some of those issues.[40]

3.31 It is also noted that the OPC is developing privacy impact assessment guidelines for public sector agencies, which the OPC considers could also be applicable in the private sector.[41] The OPC also noted that 'a wider review of the Privacy Act could consider the question of whether the Privacy Act should include provisions which provide for a privacy impact assessment to be carried out in specified circumstances.'[42]

---

38 *Committee Hansard*, 22 April 2005, p. 16.

39 *Committee Hansard*, 22 April 2005, pp 45-46. Note also that the issue of funding and resourcing of the OPC is discussed in further detail later in this report.

40 *Committee Hansard*, 19 May 2005, p. 55.

41 OPC review, p. 256.

42 OPC review, p. 256.

OPC review

3.32 The OPC review of the private sector provisions of the Privacy Act (which is discussed further in chapter 4) considered the adequacy of the private sector provisions in protecting individual privacy in light of technological developments.[43] Indeed, similar issues were raised in submissions to that review as were raised during this inquiry. The OPC made a number of recommendations to address the issue of new technologies. Among other matters, the OPC's review recommended that:

> The Australian Government should consider, in the context of a wider review of the Privacy Act (see recommendation 1) reviewing the National Privacy Principles and the definition of personal information to assess whether they remain relevant in the light of technological developments since the OECD principles were developed. This should ensure that the private sector provisions remain technologically neutral and relevant to protect data privacy in the main contexts in which information about people is currently collected, used and disclosed.[44]

3.33 The OPC review also committed to issuing:

> …further guidance, consistent with the current law, on what is personal information which takes into account the fact that in the current environment it is more difficult to assume that any information about people cannot be connected.[45]

3.34 The OPC review also noted that it had recommended new powers to develop binding codes, and that these could be used to deal with technologically specific situations.[46] The OPC's recommendation in relation to binding codes is considered further in chapter 4.

Smart cards and national identification schemes

3.35 This next section considers term of reference (a)(ii)(A), which refers to 'smart card' technology and the potential for this to be used to establish a national identification regime.

3.36 A 'smart card' is a card resembling a credit card in size and shape. Smart cards contain a built-in or 'embedded' microprocessor capable of storing data. They have a

43 OPC review, pp 239-257.

44 OPC review, Recommendation 69, p. 257.

45 OPC review, Recommendation 71, p. 257.

46 OPC review, Recommendation 73, p. 257.

potentially wide range of applications and may store a large amount of information.[47] As the LIV submitted:

> Smart Cards and the systems that support them are able to store vast amounts of information. This information may include banking details, store vouchers, Tax File Numbers, health records.[48]

3.37 Submissions noted that many overseas countries have started using smart cards for various applications, including ID cards, credit cards, health cards and driver licenses.[49] Others noted that smartcards are already in use in Australia for a range of purposes, such as bank credit cards and transport ticketing cards. For example, a number of submissions expressed concern about the Queensland government's proposal for a new Queensland driver licence using smartcard technology.[50]

3.38 There were mixed views in submissions as to whether smart cards are privacy enhancing or privacy invasive. Some submissions argued that smart card technology, depending on its design and implementation, could offer enhanced security and privacy protection.[51] Indeed, Lockstep Consulting submitted that 'greater use of smartcards is urgently required to protect the privacy of Australians.'[52] Lockstep Consulting argued that:

> One thing that makes smartcards "smart" is their ability to be programmed to make decisions about when and where they will exchange data with the outside world… These sophisticated capabilities can be used to protect card holder privacy in many different ways. In our opinion, of particular relevance to the Committee's inquiry are two unique abilities: management of multiple identifiers, and protection against website fraud such as phishing.[53]

---

47 See further Michael Walters, "Smart cards and privacy", *Privacy Law and Policy Reporter*, Vol. 1 No. 8, 1994, p. 143; Darren Baguley, "Card sharps", *The Bulletin*, v. 121 (6373), 20 May 2003, pp 68-69; See also, for example, Centre for Law and Genetics, *Submission 24*, pp 2-3; Lockstep Consulting, *Submission 11*, p. 5.

48 *Submission 37*, p. 10.

49 See, for example, Lockstep Consulting, *Submission* 11, p. 8; Sony Business Solutions, *Submission 14*, pp 1-2; see also Privacy International and Electronic Privacy Information Center, *Privacy and Human Rights 2004: an International Survey of Privacy Laws and Developments*, 2004, http://www.privacyinternational.org/survey/phr2004 (accessed 23 February 2005).

50 See, for example, ACA, *Submission 15*, pp 9-10; EFA, *Submission* 17, pp 19 and 24; LIV, *Submission 37*, p. 10.

51 See, for example, Centre for Law and Genetics, *Submission 24*, p. 3; Australian Electrical and Electronic Manufacturers' Association (AEEMA), *Submission 26*, p. 1; Lockstep Consulting, *Submission 11*, pp 2 and 5.

52 *Submission 11*, p. 1.

53 *Submission 11*, p. 5.

3.39 In contrast, other submitters expressed concern about the negative privacy implications of smart cards. For example, the Office of the Victorian Privacy Commissioner commented that, in relation to smart cards:

> The dumber the better, unless they include safeguards for privacy, accessibility to the data they hold for the data-subject, an option of anonymity where that is feasible (eg public transport smartcards, which offer terrific benefits if done well). A key question is: who controls the back office and is accountable for the subsequent use, disclosure, accuracy and security of the data gathered and distributed via smartcards?[54]

3.40 Indeed, several other submissions also stressed the need to consider appropriate access and storage arrangements in relation to data gathered and distributed via smart cards.[55] EFA also expressed concern that smartcards have 'known security flaws', arguing that 'while smart cards may be tamper-resistant, they are not tamper-proof.'[56] Other submissions were concerned about the potential use of smart cards for surveillance.[57] As the LIV submitted:

> Those in favour of Smart Cards believe that they improve customer service, operational efficiency and security for both the public and private sectors. However, the LIV suggests that Smart Cards also have the potential to become a technology of surveillance and control…[58]

3.41 Mr Bill O'Shea from the LIV was also concerned:

> …about the linking of information through smart cards. One of the problems with smart cards is that often people do not know what is actually stored on a smart card and therefore how to access what is there, nor do they know who is going to get the information on the smart card. In a sense, that was part of the concern about the Australia card as well. We would be very concerned about any inability under the [A]ct to deal with this issue to prevent that happening. There need to be strong restrictions on the use of the smart card.[59]

3.42 Some submissions also noted that the smart card industry, particularly the Asia Pacific Smart Card Forum, had developed a code of conduct requiring compliance with the NPPs.[60]

---

54 *Submission 33*, p. 4.

55 See, for example NHMRC, *Submission 20*, p. 4; LIV, *Submission 37*, p. 10; Caroline Chisholm Centre for Health Ethics, *Submission 21*, p. 5; Centre for Law and Genetics, *Submission 24*, p. 3.

56 *Submission 17*, p. 25.

57 See, for example, LIV, *Submission 37*, p. 10; also EFA, *Submission 17*, p. 23.

58 *Submission 37*, p. 10.

59 *Committee Hansard*, 22 April 2005, p. 17.

60 AEEMA, *Submission 26*, p. 1; Centre for Law and Genetics *Submission 24*, p. 3.

Function creep and national ID schemes

3.43 Some submitters were concerned about the potential for 'function creep' in the use of smart cards - that is, the tendency to use something beyond the purpose for which it was intended. Some of these submitters were particularly concerned that smart cards could be used to establish a national identification scheme.[61] For example, EFA submitted that:

> …the roll out of smart cards by government has an extremely high potential to result in the equivalent of an Australia card, whether or not that is the government's intention at the outset. This potential arises from a combination of factors including the ease with which smart cards can be used for two-way communication with a centralised database and that smart card technology is designed to facilitate function creep.[62]

3.44 EFA continued:

> Even if a smart card is rolled out as single use/purpose, or "voluntary", together with legislative and technological controls to prevent function creep, history demonstrates that such controls are likely to be over-ridden by government in the not very distant future.[63]

3.45 EFA noted that function creep of smart cards could occur, for example, in the form of additional government mandated uses of the same smart card; additional personal information being loaded onto the card; additional applications being loaded on to the smart card; or smart card readers being linked to one or more centralised databases.[64]

3.46 Submissions also noted that other countries, including the UK, are developing or have already implemented national ID smart cards.[65] However, it was observed that a national ID smart card would not be welcomed nor warranted in Australia.[66] For example, the ACA argued that it is 'naïve and dangerous to assume that a single

---

61 EFA, *Submission* 17, pp 19-23; Caroline Chisholm Centre for Health Ethics, *Submission 21*, pp 5-6 and Appendix 1.

62 *Submission 17*, p. 19.

63 *Submission 17*, p. 19.

64 *Submission 17*, p. 20.

65 See for example, AEEMA, *Submission 26*, p. 1; Sony, *Submission 14*, pp 1-2; see also Rotenberg, M. and Laurant, C., Privacy International and Electronic Privacy Information Center, *Privacy and Human Rights 2004: An International Survey of Privacy Laws and Developments*, 2004, available at: http://www.privacyinternational.org/survey/phr2004 (accessed 23 February 2005).

66 Caroline Chisholm Centre for Health Ethics, *Submission 21*, p. 5; Mr David Travis, *Submission 23*, p. 2.

authentic identity is necessary or even desirable for most consumers'.[67] Similarly, Ms Anna Johnston of the APF raised concerns with such ID proposals:

> …we do not believe an Australia Card or any centralised identity management model is the appropriate way to go. We actually think that would increase the risks rather than address them. To use the honey pot argument: the more you centralise the information the more it attracts people; it becomes more valuable for organised criminals or terrorists to hack into the database. When you centralise it they only have to hack into one database or bribe one clerk to get access to the information.[68]

3.47 Some submissions argued that existing schemes, such as driver licences, could already be considered to be the equivalent of, or contain potential for, a national ID scheme.[69] Certainly, the ACA expressed the opinion that:

> Australia does have a national identification regime today, one that serves most consumers quite well on a day-to-day basis.[70]

3.48 At the same time, the ACA acknowledged that:

> It would be naïve and complacent not to acknowledge challenges within that regime. It does seem clear that some traditional authentication documentation and credentials such as birth certificates, drivers' licenses and various commercial statements are falling prey to counterfeiting and forgery with the advent of technologies such as scanners, laser printers and colour photocopiers. In our view these challenges need to be met, not with an additional layer of electronic authentication, but by making existing processes more robust. This means designing better documents, and constructing document reference mechanisms that validate the credential in specific circumstances, without intruding unnecessarily on the personal identity of the individual holding it.[71]

3.49 Indeed, identity fraud as an invasion of privacy was a related issue raised during the Committee's inquiry. The APF welcomed debate about identity management, but was concerned that:

> … too many initiatives in the area of identity management, some involving the use of biometrics and smart cards, are being developed behind closed doors, by vested interests, and without due regard for wider social

---

67 *Submission 15*, p. 9.

68 *Committee Hansard*, 19 May 2005, p. 17.

69 See, for example, Caroline Chisholm Centre for Health Ethics, *Submission 21*, p. 5; Mr David Travis, *Submission 23*, p. 2; AEEMA, *Submission 26*, p. 1.

70 ACA, *Submission 15*, p. 7; see also Mr Charles Britton, *Committee Hansard*, 19 May 2005, p. 27.

71 *Submission 15*, pp 7-8.

> implications, including for privacy. There is far too much loose thinking around the subject of identity management.[72]

3.50 In particular, the APF suggested that the extent of identity crime is 'poorly quantified and often exaggerated.'[73] The APF came to the conclusion that:

> There is a very strong argument to be made that the separation of data in functional silos (health, taxation, transport etc) – far from being a problem – is actually one of our strongest protections against security breaches having traumatic consequences. Proponents of identity schemes, monitoring and data matching seem to proceed on the naïve assumption that their scheme can somehow be made 100% accurate and secure, despite the evidence of history, and the reality of all human systems, that errors and security breaches will inevitably occur.[74]

3.51 The proposal for a 'national document verification system', as recently reported in the media, was noted in some submissions.[75] However, EFA commented that the lack of publicly available information about the scheme made it difficult to determine privacy and security risks posed by the proposed scheme.[76]

3.52 In response to the committee's questioning on the issue, the Privacy Commissioner noted that the OPC had been working with the Attorney-General's Department on the proposed document verification service, and had been provided funding in the recent budget for that purpose.[77]

3.53 During the Senate Legal and Constitutional Legislation Committee's May 2005 Budget Estimates hearings, a representative of the Attorney-General's Department elaborated further on the proposal and gave an example of how it might work:

> Someone might present at a passport office presenting a New South Wales driver's licence as evidence of their identity. The operator at the passport office would perhaps type in a few details that appear on the driver's licence—for example, their name, their date of birth, their gender or perhaps the driver's licence number. The message would be sent electronically through a routing system to the road and transport authority of, for example, New South Wales asking them whether or not they had

72 *Submission 32*, p. 10.

73 *Submission 32*, p. 10.

74 *Submission 32*, p. 10.

75 EFA, *Submission 17*, pp 29-30; LIV, *Submission 37*, p. 11.

76 *Submission 17*, pp 29-30.

77 Ms Karen Curtis, OPC, *Committee Hansard*, 19 May 2005, p. 55; see also Attorney-General's Department, *Committee Hansard*, 19 May 2005, p. 64.

> issued a document with those details on them. Electronically, a message would come back yes or no. There is no exchange of information per se.[78]

3.54 The representative further stated that:

> The kind of procedure that would be involved in the document verification service is not dissimilar to checks that they would already be undertaking. What it aims to do and what it does do is provide an online real-time check rather than something which is a manual process.[79]

Medicare smartcard

3.55 Several submissions observed that the Australian Government has recently launched a new 'Medicare smartcard'. Medicare smartcards have been made available in Tasmania on a trial basis as the first stage of their national introduction. According to the Department of Health and Ageing, the card will be voluntary, and will support the current uses of the Medicare card. The Department submitted that the chip on the Medicare smartcard will also contain a consumer identifier, and basic demographic and other patient information if required. The Department noted that the use of the Medicare smartcard is governed by existing provisions of the Privacy Act.[80]

3.56 A number of submissions raised privacy concerns in relation to the Medicare smartcard.[81] The Australian Medical Association (AMA) raised concerns about the consumer identification number being embedded in the card, and the fact that there appeared to be no stated purpose for that number.[82] Ms Julia Nesbitt explained to the Committee:

> …there has still been no discussion on what the purpose of that chip is and what the purpose of that number is. It goes to the issue of the development of a unique patient identifier—the key to protection of an individual's privacy and their understanding of their rights under the Privacy Act. There must be a purpose associated with that number so the limits of the use of that number can be understood.[83]

3.57 Ms Irene Graham from EFA suggested that the Medicare smartcard trial should be discontinued until further work has been carried out:

> …we do not necessarily oppose the use of the smart card, but we would like to see evidence that there is a reason to use a smart card and there is no potentially less privacy invasive method of achieving the same objective.

---

78 *Estimates Hansard,* 23 May 2005, p. 86.

79 *Estimates Hansard,* 23 May 2005, p. 87.

80 *Submission 34*, pp 13-14.

81 See for example, LIV, *Submission 37*, p. 10; AMA, *Submission 9*, p. 6; EFA, *Submission 17*, pp 22-24.

82 *Submission 9*, p. 6; see also LIV, *Submission 37*, p. 10.

83 *Committee Hansard*, 20 May 2005, p. 16.

> Our core concern with the Medicare smart card proposal at the moment is that there is simply no information at all that explains why a smart card is needed or how it is going to be used to protect privacy and security of people's information. All indications to us at the moment are that it is basically going to have completely the opposite effect…we think the Medicare smart card roll-out should be halted until there has been a proper assessment of and justification for it.[84]

3.58 In particular, Ms Irene Graham suggested more specific laws may be needed in context of proposals like the Medicare smartcard:

> …if things like smart cards are going to be used for Medicare with these databases where you can access your personal information, instead of just having high level principles we need actual law that says the only people who can access the back-end database are this organisation or this government department or this set of people, instead of guidelines that just broadly say, 'If it is necessary to have access, then you can have access' and exemptions to the privacy principles that are very broad by saying that law enforcement can access information if it is necessary for the investigation of some law. We do not believe that those kinds of very broad exemptions should apply to people's medical and health information that would be in a Medicare smart card kind of arrangement.[85]

3.59 EFA suggested that, at the very least, an independent privacy impact assessment of the smartcard should be conducted, and that security measures should be built into the smartcard.[86]

3.60 The AMA noted that the Medicare smartcard was announced 'without any consultation with the wider community.'[87] Ms Nesbitt of the AMA argued that there should be:

> …strong consultation should the smartcard be the solution that the government ultimately accepts...They were talking about all sorts of things being on the card—for instance, allergies. It is not good clinical practice for a patient to go into Medicare and say, 'I'm allergic to this and allergic to that.' It needs really close consultation with the medical profession about what should be on it. What is the most important information, what is really necessary, from a clinical perspective, should be on the card.[88]

3.61 When questioned by the committee on the consultation undertaken in relation to the Medicare smartcard, the Department of Health and Ageing responded that:

---

84 *Committee Hansard*, 22 April 2005, p. 46.

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

86 *Submission 17*, p. 24.

87 *Submission 8*, p. 6.

88 *Committee Hansard*, 20 May 2005, p. 22; also pp 16, 21.

> Six Consumer Focus Testing sessions were held in June 2004 to understand attitudes and expectations about the use of the smartcard prior to its release.[89]

3.62 The Department of Health and Ageing also noted that that government agencies and providers had also been consulted, and that:

> In-depth consultation took place with consumer representative groups and consumer focus groups. Consumer groups consulted were Consumers' Health Forum, Chronic Illness Alliance, Health Consumers Rural and Remote Australia, Australian Federation of Disability Organisations and the Health Issues Centre.[90]

3.63 In response to the committee's questioning on the Medicare smartcard, the OPC noted that it had provided advice on the proposed smartcard.[91] For example, the OPC had advised that protections against, and restrictions on, 'function creep', including a clear articulation of the purpose of the card, will be necessary in gaining community and stakeholder confidence. It also noted that the Medicare smartcards are intended to be voluntary and individuals without them should not be disadvantaged.[92]

3.64 EFA were sceptical about the voluntary nature of the smartcard, arguing that while the card may be optional initially:

> The next stage would occur in a few years when the remaining members of the public who had declined to opt in would be told that it has become too costly, or impractical, to continue with two different cards so the smart card and reliable national identification number has become mandatory. Thereafter it is a relatively simple matter to add new applications to the card, as just one example, to control the types of purchases that may be made with welfare payments.[93]

3.65 Indeed, several submitters raised concerns about the potential for function creep in relation to the Medicare smartcard. EFA suggested that it has high potential to result in the equivalent of an Australia Card.[94] EFA argued that the Medicare smartcard:

> …seems likely to become requested, or required, as a *primary* proof of identity document…Whether this will occur will depend on whether a

89 *Submission 34B*, p. 2.

90 *Submission 34B*, p. 2.

91 Ms Karen Curtis, OPC, *Committee Hansard*, 19 May 2005, p. 55; see also *Submission 48*, p. 14.

92 *Submission 48*, p. 14.

93 *Submission 17*, p. 23.

94 EFA, *Submission 17*, pp 19 and 22-23.

> card's chip contains the "optional" photograph/s and of course whether the inclusion of photographs remains optional.[95]

3.66 Others expressed concern about the use of the Medicare smartcard for other purposes, including welfare related purposes.[96] For example, Mr Bill O'Shea from the LIV noted that:

> Just yesterday we saw Minister Hockey making an announcement about the possible use of smart cards to link this information. We believe that is inappropriate and we would oppose it. We are not saying that we therefore support welfare fraud. We are saying that there is a more fundamental issue at stake here and that is that smart cards should be used sparingly and only to the extent that it is absolutely necessary.[97]

3.67 However, the Department of Health and Ageing stated that 'there is no intention to widen the use of the Medicare smartcard or identifier beyond the health sector.'[98] When questioned further by the committee on this issue, representatives from the Department of Health and Ageing responded that the extension of the Medicare smartcard to use by other agencies such as Centrelink was not under consideration by the Department and that:

> From the perspective of our department, at this stage there is no intention for the function of the HealthConnect card to be wider than health information.[99]

3.68 However, the committee notes that Cabinet has recently approved a proposal by the Minister for Human Services, the Hon. Joe Hockey MP, to expand the use of the Medicare smartcard by linking it to other Government services, including welfare services.[100] Minister Hockey has explained that "what the smartcard represents is one set of keys to open a number of doors to a range of government services and benefits".[101]

Biometrics

3.69 The term 'biometrics' refers to a range of measures of biological data. Biometric information can include fingerprints, retina/iris scans, hand geometry, facial scans, voice recognition, DNA samples, and digitized (electronically stored)

---

95 *Submission 17*, p. 22.

96 See, for example, Ms Irene Graham, EFA, *Committee Hansard*, 22 April 2005, pp 48-49; Mr Bill O'Shea, LIV, *Committee Hansard*, 22 April 2005, p. 17.

97 *Committee Hansard*, 22 April 2005, p. 17; see also Misha Schubert, "New smartcards could keep track of welfare", *The Age*, 21 April 2005, p. 3.

98 Department of Health and Ageing, *Submission 34*, p. 14.

99 *Committee Hansard*, 20 May 2005, pp 32-33 cf OPC, *Submission 48*, p. 15.

100 "Privacy fears over health, welfare card", *Australian Financial Review*, 16 June 2005, p. 3.

101 "New smartcards could keep track of welfare", *The Age*, 21 April 2005, p. 3.

images.[102] Some submissions therefore suggested that the inquiry's terms of reference, which refer to 'biometric imaging data', should include biometric data more generally.[103]

3.70 There were mixed views as to whether biometric information would be covered under the current Privacy Act, and whether the use of biometrics is privacy enhancing or privacy invasive.[104] The APF acknowledged that biometrics could be privacy enhancing when used to provide security against unauthorised access to other personal information. At the same time, the APF was concerned that biometric technology could be privacy intrusive, for example, when used to monitor an individual's movements or activities.[105] Some submitters believed that the greatest threat to privacy would arise through the storage of biometric data.[106]

3.71 Some submissions expressed concern about the reliability and vulnerability of the technology associated with biometric data.[107] For example, the LIV suggested that:

> The biometric encryption system is vulnerable and highly susceptible to be infiltrated by hackers. Subsequently the system is not secure.[108]

3.72 Mr Bill O'Shea from the LIV elaborated on this during the Committee's hearing in Melbourne:

> In terms of biometric encryption, we do not believe the technology is secure. If the technology was secure, we would be more comfortable about biometric encryption being used. However, we believe it is still subject to hackers and interception, and we urge caution in terms of allowing biometric encryption in Australia until that technology improves further.[109]

---

102 See further Malcolm Crompton, "Biometrics and Privacy", *Privacy Law and Policy Reporter*, vol 9, no 3, July 2002, pp 53-58; and vol 9 no 4, August 2002, pp 68-73.

103 ACA, *Submission 15*, p. 12; Dr Anthony Place, *Submission 22*, p. 4.

104 Department of Health and Ageing, *Submission* 34, pp 16-17; cf Sony Business Solutions, *Submission 14*, p. 2; also Caroline Chisholm Centre for Health Ethics, *Submission 21*, p. 7, and Attachment 2; APF, *Submission 32*, Annex D, p. 1; Roger Clarke, *Submission 28*. See further Malcolm Crompton, "Biometrics and Privacy", *Privacy Law and Policy Reporter*, vol 9, no 3, July 2002, p. 54.

105 *Submission 32*, Annex D, p. 1.

106 AEEMA, *Submission 26*, p. 2; see further Malcolm Crompton, “Biometrics and Privacy: The end of the world as we know it or the white knight of privacy?” *Australian Journal of Forensic Sciences*, vol 36, 2004, pp 49-58.

107 ACA, *Submission 15*, p. 12; Lockstep Consulting, *Submission 11*, pp 2, 12-19; LIV, *Submission 37*, p. 11.

108 *Submission 37*, p. 11.

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

3.73 Several submitters were also concerned that once biometric data has been compromised or stolen, it is very difficult to rectify the problem.[110] For example, Lockstep Consulting observed that 'most biological traits can in fact be duplicated with sufficient fidelity to fool most biometric detectors.'[111] Lockstep Consulting continued:

> …the critical question is: What are we to do in the event that an individual's biometric identity becomes compromised? We know what do when any other authenticator is stolen, be it a password, a magnetic stripe card, or a smartcard: we simply revoke it and issue a new one. But as things stand today, no biometric identifier can be cancelled and re-issued. In the event of biometric identity theft, there would appear to be no alternative but to withdraw the affected user from the system.[112]

3.74 Similarly, the Australian Electrical and Electronic Manufacturers' Association (AEEMA) noted that 'once stolen, a biometric is stolen for life.'[113]

3.75 The Office of the Victorian Privacy Commissioner suggested that privacy impact assessments should be conducted before differing biometric devices are introduced.[114] Similarly, the National Health and Medical Research Council (NHMRC) recommended that there should be extensive public consultation in relation to the use of biometric imaging.[115]

Biometric Passports

3.76 The Department of Foreign Affairs and Trade (DFAT) submitted details of the proposed introduction by 26 October 2005of facial biometrics into all Australian passports.[116] This proposal follows the adoption of facial recognition as the global standard for biometric identifiers in passports by the International Civil Aviation Organisation (ICAO). Further, from October 2005, the United States (US) will require travellers from its Visa Waiver Program countries to have introduced a biometrics passports system.[117]

---

110 Caroline Chisholm Centre for Health Ethics, *Submission 21*, p. 7; Lockstep Consulting, *Submission 11*, p. 18.

111 *Submission 11*, p. 18.

112 *Submission 11*, p. 18.

113 *Submission 26*, p. 2.

114 *Submission 33*, p. 4.

115 *Submission 20*, p. 5.

116 The proposal is still subject to government approval: DFAT, *Submission 39*, p. 3. There has also been some discussion about the October deadline being extend: DFAT, *Committee Hansard*, 20 May 2005, p. 2.

117 DFAT, *Submission 39*, pp 2-3; see also Morag Donaldson, *Australian Passports Bill 2004*, Parliamentary Library Bills Digest No. 75-77. 2004-2005, 7 December 2004, p. 5.

3.77 DFAT submitted that the introduction of facial biometric technology into Australian passports is 'as much about protecting the privacy of passport holders as it is about improving the security of the process.'[118] DFAT explained in its submission that, under the proposed new passport system, the biometric information obtained from an individual's passport photograph will be stored in a contactless chip embedded in the passport.[119] DFAT submitted that the information sought from applicants will remain the same – that is, a photograph. DFAT argued that 'the only change is that the individual will be matched to an image of themselves by a machine rather than a person.'[120] A representative of DFAT explained to the Committee that the chip on the passport will contain:

> Only the information that is currently shown on the data page. The suggestion that biometric data is something different is probably one of the greatest misunderstandings in relation to the introduction of this technology. It is simply what we now have on the data page of the passport. The only difference is it is written to the chip as well.[121]

3.78 The representative of DFAT elaborated on this:

> …what is being proposed is nothing different, really, to what exists currently. There is no more data involved in the e-passport process. There is no more data held centrally on Australian citizens than there is currently. We currently have biodata. We have all of the personal details of Australian passport applicants. We currently have images on our passport databases. Those things would remain under the e-passports project.[122]

3.79 The use of facial biometrics in passports will be regulated under the *Australian Passports Act 2005* (Passports Act), which commences on 1 July 2005. The Passports Act enables the Minister to determine particular methods and technologies that can be used to confirm 'the validity of evidence of the identity of an applicant for an Australian travel document'. Any determination relating to the use of personal information must specify the nature of the personal information and the purposes for which it may be used.[123]

3.80 DFAT submitted that 'it is the Government's intention to implement the new [Passports] Act in a manner consistent with the privacy principles and policies embodied in the Privacy Act 1988.'[124] DFAT also submitted that the Minister's

---

118 *Submission 39*, p. 1.

119 *Submission 39*, p. 2.

120 *Submission 39*, p. 1.

121 *Committee Hansard*, 20 May 2005, p. 3.

122 *Committee Hansard*, 20 May 2005, p. 4.

123 Section 47. Note that a determination under section 47 will be a disallowable instrument; see also DFAT, *Submission 39*, pp 3-4.

124 *Submission 39*, p. 1.

determination will be 'underpinned by a Privacy Impact Assessment which will be subject to scrutiny by the Office of the Federal Privacy Commissioner'.[125]

3.81 In response to the committee's questioning on to the extent to which privacy impact assessment had been, or was being, conducted in relation to the biometric passports, a representative of DFAT replied:

> There have been two privacy impact assessment projects conducted so far. One was done prior to the introduction into parliament of the legislation. That was done last year. That privacy impact assessment of course included the provisions relating to the introduction of biometric technology into Australian passports. And there is currently a biometrics- or e-passports-specific privacy impact assessment being prepared.[126]

3.82 The representative noted that the assessment was being prepared 'internally in consultation with privacy advocates and the Privacy Commissioner'.[127]

3.83 Indeed, the OPC noted that it had provided advice on the passports legislation, and that this advice had been 'taken on board'.[128] Further, it was noted that the Privacy Commissioner had been funded in the recent budget 'to work with Customs and DIMIA [Department of Immigration and Multicultural and Indigenous Affairs] and DFAT on biometrics.'[129]

3.84 However, EFA advised that they believed that any privacy protection afforded by the Privacy Act in this context was likely to be 'weak at best'. In particular, EFA was concerned that any disclosure pursuant to a determination made by the Minister under the Passports Act would be 'authorised or required by law' and therefore fall within the category of disclosure to which the Privacy Act does not apply.[130]

3.85 Some submitters were also concerned that the chip to be implanted in passports could be read remotely, and that this could actually facilitate identity theft.[131] For example, Mr Roger Clarke described the passports proposal as 'naïve and dangerous', arguing that placing enormously sensitive data into an RFID tag, including biometrics will facilitate identity theft.[132]

---

125 *Submission 39*, p. 4.

126 *Committee Hansard*, 20 May 2005, p. 2.

127 *Committee Hansard*, 20 May 2005, p. 2.

128 Mr Timothy Pilgrim, OPC, *Committee Hansard*, 19 May 2005, pp 55-56.

129 Ms Karen Curtis, OPC, *Committee Hansard*, 19 May 2005, p. 55.

130 *Submission 17*, p. 29.

131 EFA, *Submission 17*, pp 27-28; Mr Roger Clarke, *Submission 28*, p. 2.

132 *Submission 28*, p. 2.

3.86 In a similar vein, EFA argued that 'the particular type of computer chip to be implanted in passports is also a danger to individuals' security and privacy'.[133] According to EFA:

> The information on the chips can be read remotely by anyone with any reader, not just by the reader to be used by immigration/customs officials.[134]

3.87 During the committee's hearing in Canberra, a representative from DFAT responded to this suggestion:

> We are very aware of the concerns of not only privacy advocates but a number of others within the community, in Australia and internationally, particularly in the United States, about this possibility of eavesdropping—the illegal reading of passport data contained on microchips—or skimming, as it is commonly known. We have looked at this quite extensively and our testing to date has failed to prove that it is a possibility, frankly. But it remains a very strong perception and we have taken the view that, in the longer term at least, it will be possible to do it. So to mitigate that possibility we have decided to introduce a coded arrangement, called basic access control, which will require that the machine-readable zone on the data page of the passport be read in order to unlock the chip—in other words, the data on the chip will be protected and will not be able to be read unless that pin is used to unlock it.[135]

3.88 The ACA was concerned about the reliability of biometric technology, and the 'possible expanded use of the credential in Australia rather than as a travel document in and out of Australia.'[136] For example, the ACA observed that the reference material about biometrics provided by DFAT noted that some of the reasons for an incorrect or low scoring match included, for example, a smile with teeth showing, hair over the face, non-centred pose, or glasses with dark tint. ACA submitted that:

> This has resulted in new passport photo guidelines being developed to ensure submitted passport photos will provide the best possible performance for biometric matching. In the worst sort of technology push imaginable, we face the prospect of a requirement for citizens to submit unsmiling to imaging procedures, wearing standardised spectacles, with government standard haircuts, in a special official pose – a prescription that seems more suited to North Korea than to Australia.[137]

3.89 A representative of DFAT responded to these concerns:

---

133 *Submission 17*, p. 27.

134 *Submission 17*, p. 27; see also ACA, *Submission 15*, p. 14.

135 *Committee Hansard*, 20 May 2005, pp 2-3.

136 *Submission 15*, p. 12.

137 *Submission 15*, p. 13; see also Ms Irene Graham, *Committee Hansard*, 22 April 2005, p. 50; EFA, *Submission 17*, pp 28-29.

> It is, of course, correct that, with ageing, simple things like hair covering foreheads, beards and glasses and so on can have impacts on this technology. I think the important thing to note is that we have done a lot of testing with regard to those issues. Because this technology is based on what we call eye coordinates, we have been able to do a lot of work within the software to ensure that we can get matches about 98 per cent of the time. As far as the other two per cent are concerned, all that happens, if somebody has got older and cannot be matched, is that they will simply be referred to a secondary processing at airports, for example, to ensure that they are who they claim to be. I think there is some misunderstanding that individuals will suffer as a result of perhaps not having been matched…It is generally accepted the way those people will be processed is simply the way they are processed now. The data on the microchip is designed to facilitate the processing of people through matching.[138]

Draft Biometrics Privacy Code

3.90 Some submissions noted that the Biometrics Institute (an independent organisations for users of biometric services and products)[139] had prepared a draft privacy code of practice, which has been submitted to the OPC for registration as a code of practice for the biometrics 'industry' under Part IIIAA of the Privacy Act.[140] The APF and the ACA expressed some concern about this proposal. In particular, the APF noted that, for many organisations the proposed biometrics code would only apply to a small part of their full range of activities. Any activities that did not involve the use of biometrics would remain subject to the NPPs, and it would be difficult to draw a clear distinction in most biometric applications.[141]

3.91 ACA expressed a more general concern about the use of codes to cover technologies, rather than industries:

> In our view Codes were envisaged by the legislation as applying to industries, or more narrowly to parts of industries or even organisations. This could be characterised as a 'vertical' orientation. The development of codes to cover technologies that might be used by any number of industries could be characterized as 'horizontal'.

3.92 Some of the ACA's concerns in relation to this 'horizontal orientation' of industry codes included that companies would need to understand the circumstances in which the technologically specific code would apply and the boundaries to that in their operations. The ACA also noted that this approach could result in companies

---

138 *Committee Hansard* , 20 May 2005, p. 3.

139 See further www.biometricsinstitute.org

140 See, for example, ACA, *Submission 15*, pp 11-12; APF, *Submission 32*, Annex D; LIV, *Submission 37*, p. 5; Victorian Privacy Commissioner, *Submission 33*, p. 4; see further: http://www.privacy.gov.au/business/codes/index.html#3 (accessed 16 April 2005).

141 *Submission 32*, Annex D, p. 2; see also ACA, *Submission 15*, p. 11.

being subject to a number of codes, which would need to be consistent.[142] Finally, the ACA was concerned that:

> The granting of Code registration may well be taken as an imprimatur to the further deployment of a technology, when this is not the function or purpose of the Code. The OFPC does not have the resources or expertise to approve technologies for deployment into the Australian market – it should not be required to act as if it did.[143]

3.93 In the context of the proposed biometrics code, the ACA observed:

> Many organisations that might use biometric technologies would be covered by Privacy Codes that relate to their specific vertical industry (such as direct marketing, insurance or banking) and certainly be covered by the default OFPC arrangements. Hence the Biometric Code may cover a certain part of a transaction, but other portions would be subject to the generic arrangements. This would not produce certainty or simplicity for either consumer or company.[144]

3.94 However, as noted earlier in this chapter, the OPC's review of the private sector provisions recommended new powers to develop binding codes, and suggested that these biding codes could be used to deal with technologically specific situations.[145] The OPC's recommendation to consider binding codes is considered further in chapter 4.

Genetic testing and discrimination

3.95 The inquiry's term of reference (a)(ii)(c) requires the committee to consider the capacity of the Privacy Act to respond to genetic testing and the potential disclosure and discrimination of genetic information. This issue has been the subject of recent comprehensive inquiry and report by the Australian Law Reform Commission (ALRC) and the Australian Health Ethics Committee (AHEC) of the NHMRC. This section does not intend to repeat all the issues, concerns and recommendations raised during that inquiry, but will merely summarise the key recommendations and the response to, and implementation of, that inquiry to date.

3.96 It is noted that the debate on genetic privacy and discrimination has been underway in Australia for some time now. In March 1999, the Senate Legal and Constitutional Legislation Committee considered the issue of genetic privacy in its inquiry into the Genetic Privacy and Non-discrimination Bill 1998, which was

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

143 *Submission 15*, p. 2.

144 *Submission 15*, p. 11.

145 OPC review, Recommendation 73, p. 257.

introduced by Senator Natasha Stott Despoja.[146] That Bill was modelled on US legislation.[147] That inquiry recommended that the Bill not proceed, pending the further examination of a number of issues.[148]

3.97 That inquiry was followed by the inquiry and report on the protection of human genetic information in Australia by the ALRC and NHMRC.[149] As Professor Chalmers of the Centre for Law and Genetics observed:

> Without the introduction of the original genetic discrimination legislation in the Senate…I am not sure that this country would have moved quite so quickly towards the establishment of the ALRC recommendations. I think it has spurred our attention.[150]

3.98 The ALRC and NHMRC report, entitled *Essentially Yours,* was published in March 2003. As Professor David Weisbrot of the ALRC explained to the Committee, this inquiry considered three key matters relating to the protection of human genetic information, and in particular: privacy protection; unlawful discrimination and ethical standards.[151] Professor Weisbrot further explained that:

> We then took that across a very wide array of subject matter, including those in the medical and health area, like clinical research, the deliverance of clinical services, public health administration, genetic databases and so on. On the more medical legal side, we looked at issues of insurance, immigration, employment, the use in sport, the delivery of services and a range of other issues, including identity testing, whether that was done for parentage purposes or the potential—I think harmful potential—in using it to determine race or ethnicity in the case of Aboriginality, and a range of related matters. The privacy concerns, as I said, were looked at in a wide array of contexts.[152]

3.99 The ALRC and NHMRC report concluded that legislative issues relating to genetic information are best addressed through existing legislation such as the Privacy Act, rather than a new regulatory framework dedicated specifically to the protection of

---

146 Senate Legal and Constitutional Legislation Committee, *Provisions of the Genetic Privacy and Non-discrimination Bill 1998*, March 1999. Note that the Bill still stands on the Senate Notice Paper, having been restored to the Notice Paper after each Federal election that has occurred since the Bill was originally introduced.

147 Senate Legal and Constitutional Legislation Committee, *Provisions of the Genetic Privacy and Non-discrimination Bill 1998*, March 1999, p. 1.

148 Senate Legal and Constitutional Legislation Committee, *Provisions of the Genetic Privacy and Non-discrimination Bill 1998*, March 1999, p. 39.

149 ALRC and NHMRC, *Essentially Yours: Protection of Human Genetic Information in Australia,* ALRC 96, 2003; see also ALRC *Submission 18*, p. 2; and NHMRC, *Submission 20*, p. 6.

150 *Committee Hansard*, 20 May 2005, p. 10.

151 *Committee Hansard*, 19 May 2005, p. 37.

152 *Committee Hansard*, 19 May 2005, p. 37.

genetic information.[153] Many submitters were supportive of this approach.[154] For example, Mr Bill O'Shea from the LIV agreed:

> ...we would not see separate legislation being required on this issue. I do not think the current legislation we have in Australia protects us in this area because I do not think it specifically includes the express prohibitions against it that we are suggesting. It does not necessarily have to be directed at employers or insurers; I think it is a matter of an individual's genetic information being the property of that individual and therefore it needs their consent before it can be disclosed. That way it is applicable to anyone who wishes to have access to it. There can be exceptions. …. The default position ought to be that that information cannot be used without the consent of the individual, and I think that can be done by amending the existing act.[155]

3.100 Similarly, the Anti-Discrimination Board of New South Wales expressed its view that:

> …discrimination on the basis of genetic information is not so fundamentally different from other forms of discrimination that it cannot be adequately addressed under the existing privacy and anti-discrimination legislation framework, state and federal.[156]

3.101 Many submissions expressed concern that genetic information is not currently adequately protected under the Privacy Act, or that at the very least, clarification of the Privacy Act is required.[157] For example, the Anti-Discrimination Board of New South Wales submitted that:

> Rather than acting as an impediment to the development and application of genetic technology, effective anti-discrimination and privacy legislative regimes are critical to realising the public health benefits of genetic discrimination.[158]

3.102 The ALRC's submission to this inquiry summarised some of the key recommendations relating to the Privacy Act made in the *Essentially Yours* report, including:

---

153 ALRC, *Submission 18*, p. 2.

154 See, for example, Centre for Law and Genetics, *Submission 24*, p. 5; Professor Don Chalmers, Centre for Law and Genetics, *Committee Hansard*, 20 May 2005, p. 8; Anti-Discrimination Board of NSW, *Submission 12*, p. 3; APF, *Submission 32*, p. 12; OPC, *Submission 48*, p. 9.

155 *Committee Hansard*, 22 April 2005, pp 19-20.

156 *Submission 12*, p. 3.

157 See, for example, Office of the Victorian Privacy Commissioner, *Submission 33A*, pp 1-2; Anti-Discrimination Board of New South Wales, *Submission 12*, pp 5-6; ALRC, *Submission 18*, pp 2-8; Caroline Chisholm Centre for Health Ethics, *Submission 21*, pp 7-10.

158 *Submission 12*, p. 3.

- amendment of the definitions of 'health information' and 'sensitive information', expressly to include human genetic information about an individual (Recommendations 7-4, 7-5);
- extension of the definition of 'health information' to include information about an individual who has been dead for 30 years or less (Recommendation 7-6);[159]
- extension of the coverage of the Privacy Act to all small business operators that hold genetic information or samples (Recommendation 7-7);
- extension to cover identifiable genetic samples (Recommendations 8-1, 8-2);
- creation of a right of an individual to access his or her own body samples for the purpose of medical testing, diagnosis or treatment (Recommendation 8-3);
- creation of a right of an individual to access genetic information or body samples of his or her first-degree genetic relatives, where such access is necessary to lessen or prevent a serious threat to his or her life, health or safety (Recommendations 8-4, 21-3);
- permission for a medical professional to disclose genetic information about his or her patient to a genetic relative, where this disclosure is necessary to lessen or prevent a serious threat to an individual's life, health or safety (Recommendation 21-1); and
- amendments to ensure that employee records containing genetic information are subject to the protections of the Privacy Act (Recommendations 34-1, 34-2).[160]

3.103 In relation to the amendment to the definitions of 'health information' and 'sensitive information' to refer specifically to genetic information, the ALRC's submission noted that:

> …genetic information should receive the heightened protection afforded to health and other sensitive information under the Privacy Act, but that the existing definitions of health information and sensitive information do not provide the desired level of protection for all genetic information. There are circumstances in which genetic information may not amount to 'health information'—either because the information is not about health, disability or the provision of a health service (as in the case of parentage or forensic testing, where the focus is on identification), or because it is not about the health or disability of an existing individual (as sometimes may be the case with genetic carrier testing, where the information is primarily about the health of future children).[161]

159 See also APF, *Submission 32*, p. 15; Department of Health and Ageing, *Submission 34*, p. 21.

160 *Submission 18*, pp 2-3; see also Professor David Weisbrot, ALRC, *Committee Hansard*, 19 May 2005, p. 43; NHMRC, *Submission 20*, p. 6.

161 *Submission 18*, p. 3; see also Professor David Weisbrot, ALRC, *Committee Hansard*, 19 May 2005, p. 43.

3.104 As to the coverage of genetic samples, the ALRC noted in its submission that:

> The Inquiry concluded that the Privacy Act does not currently cover genetic samples, even where these are identifiable to an individual (eg, the container has a name or identifier attached)… There was broad support for extension of the Privacy Act to cover identifiable genetic samples in the submissions and in the extensive national consultations conducted by the Inquiry partners.[162]

3.105 Some submissions to this inquiry expressed caution about these issues. For example, the Queensland Institute of Medical Research also suggested that the term 'genetic testing' should be very carefully defined in any amendments to Privacy Act.'[163] The National Serology Reference Laboratory submitted its concerns that any future changes to the Privacy Act should not introduce restrictions or processes which might interfere with its access to required samples.[164]

3.106 However, the ALRC noted that the *Essentially Yours* report identified a number of reasons for protecting genetic samples under privacy legislation, including that:

> • genetic samples are closely analogous to other sources of personal information that are covered by the Privacy Act and should be protected by rules that are consistent with those applying to the genetic information derived from samples;
>
> • there are gaps in the existing framework for protecting the privacy of individuals from whom genetic samples are taken or derived;
>
> • these gaps may be remedied if the National Privacy Principles (NPPs) or a set of similar privacy principles were to apply to genetic samples; and
>
> • no circumstances have been identified in which applying the Privacy Act to genetic samples would lead to adverse consequences for existing practices involving the collection and handling of genetic samples.[165]

3.107 Professor Weisbrot of the ALRC noted that:

> We thought that bringing the Privacy Act into the lab in that way, by coverage of samples, would work. I should say we initially had some resistance from researchers, who threw up their arms: they were already overregulated. When we talked to the people who run good labs, though, and we went through their processes, the end result was that they did not have to do anything differently. If you run a good, clean, ethical lab, you keep records properly and you are sensitive to issues of privacy and

---

162 *Submission* 18, pp 4-5; see further Chapter 8 of the ALRC *Essentially Yours* report; see also Professor David Weisbrot, ALRC, *Committee Hansard*, 19 May 2005, p. 43.

163 *Submission 13*, p. 3.

164 *Submission 5*, p. 2.

165 *Submission* 18, p. 5; see also Professor David Weisbrot, ALRC, *Committee Hansard*, 19 May 2005, p. 43.

> confidentiality, you would not have to do anything differently. I am sure it is the same in other aspects of industry. If you are doing your job properly, you do not worry about the Privacy Act.[166]

3.108 The ALRC also noted that its inquiry expressed very serious concern about the potential for non-consensual collection and analysis of DNA samples. Professor Weisbrot observed that there is currently little legal protection against such testing:

> …it is still technically possible and it is getting easier, in the absence of legal regulation, for that genetic testing to occur because the material is so readily obtainable and the costs of genetic testing are going way down.[167]

3.109 The ALRC therefore recommended a new criminal offence to prohibit an individual or a corporation from submitting another person's sample for genetic testing, or conducting such testing, without the consent of the person concerned or without other lawful authority.[168] Professor Weisbrot explained to the Committee:

> We felt so strongly about the integrity of the individual to be free from non-consensual testing—and, I should emphasise, not only in the parentage area but across the board, whether it is an insurance company, government, the media or others—that we recommended the implementation and establishment of a new crime of taking someone else's DNA and submitting it for testing without that person's consent or without other lawful authority. The other lawful authority could be an order from the Family Court or another court that orders paternity testing or it could be a statutory authority where a law enforcement officer has to take DNA samples for the purposes of a criminal investigation or it could be research that is being done under a Human Research Ethics Committee approved process. But we felt that surreptitious testing should be sanctioned.[169]

3.110 Professor Weisbrot noted that the United Kingdom parliament was currently considering legislation with a similar provision prohibiting such non-consensual genetic testing.[170]

3.111 Parentage testing was another issue considered in the ALRC's report – that is, DNA testing for the purpose of determining parentage or kinship.[171] The report made a number of recommendations, including, for example, that DNA parentage testing should be conducted only by accredited laboratories, operating in accordance with the specific accreditation requirements. The report also recommended that parentage

---

166 *Committee Hansard*, 19 May 2005, p. 44.

167 *Committee Hansard*, 19 May 2005, p. 42.

168 *Submission 18*, p. 8.

169 *Committee Hansard*, 19 May 2005, p. 41.

170 *Committee Hansard*, 19 May 2005, p. 41.

171 See also Office of the Victorian Privacy Commissioner, *Submission 33A*, p. 2.

testing reports should be inadmissible in proceedings under the *Family Law Act 1975* unless the testing complies with the *Family Law Regulations 1984*.[172]

Genetic discrimination

3.112 Several submissions expressed concern about genetic discrimination, particularly in the insurance and employment context.[173] For example, the Cancer Council of New South Wales submitted that:

> The access to and use of genetic information by insurers is a matter which has a clear concern for us. We believe the current state of research with genetics in many conditions, including cancer, still has a high level of uncertainty and hence risk assessment used in underwriting will not be accurate. Accordingly the collection of genetic information by the insurance industry should still be subject to restriction.[174]

3.113 The Cancer Council of New South Wales noted that the Investment and Financial Services Association (IFSA) has a genetic testing policy, which is an agreement between life insurers that they will not require applicants for life insurance to undergo a genetic test. The agreement, approved by the Australian Competition and Consumer Commission, has been in force since November 2000 and was extended for two years from December 2003 until December 2005.[175] The Cancer Council of New South Wales suggested that this policy should remain in place indefinitely.[176]

3.114 The Centre for Law and Genetics noted that it had been funded by the Australian Research Council for a 'Genetic Discrimination Project', which had so far 'identified about 24 or 25 genuine cases where genetic information has been used in a discriminatory fashion.'[177]

3.115 The *Essentially Yours* report recommended that the *Disability Discrimination Act 1992* be amended to clarify that the legislation applies to discrimination based on genetic status (recommendation 9-3).[178] The Anti-Discrimination Board of New South Wales supported this recommendation in its submission:

> Although in the Board's view the current definitions of disability in both the ADA [*Anti-Discrimination Act* 1977 (NSW)] and the *Disability*

---

172 *Essentially Yours* report, Chapter 35, especially Recommendations 35-1 to 35-12, pp 860-910; see also Professor David Weisbrot, ALRC, *Committee Hansard*, 19 May 2005, pp 40-41.

173 Caroline Chisholm Centre for Health Ethics, *Submission 21*, p. 10; Cancer Council of NSW, *Submission 2*, pp 3-4; Anti-Discrimination Board of NSW, *Submission 12*, p. 2; LIV, *Submission 37*, pp 12-13; Mr Bill O'Shea, LIV, *Committee Hansard*, 22 April 2005, p. 15.

174 *Submission 2*, p. 4.

175 *Submission 2*, p. 3.

176 *Submission 2*, p. 4.

177 Professor Don Chalmers, *Committee Hansard*, 20 May 2005, p. 11.

178 *Essentially Yours,* p. 312; see also the Anti-Discrimination Board of NSW, *Submission 12*, p. 2.

> *Discrimination Act 1992* (Cth) cover genetic discrimination, there is a strong public interest rationale for making such coverage explicit in all state/territory anti discrimination legislation.[179]

3.116 The committee notes that the Productivity Commission's recent review of the *Disability Discrimination Act 1992* made a similar recommendation that the definition of 'disability' in section 4 of the *Disability Discrimination Act 1992* should be amended to ensure that it is clear that it includes genetic predisposition to a disability that is otherwise covered by the Act.[180]

Response to the Essentially Yours report

3.117 Many submissions were supportive of the *Essentially Yours* report and the implementation of its recommendations.[181] Professor David Weisbrot of the ALRC noted that the ALRC's report had been well received overseas:

> It has probably been the ALRC's biggest hit overseas, in part because the issues involved are so international; it is not looking at an area of local law. It has been used very extensively by Health Canada, which is the department of health there. The OECD working group on human genetic research databases and their working group on genetic testing are both using it very extensively. The Human Genome Organisation's ethics committee and UNESCO's bioethics committee are both referring to it regularly. The Japanese government, the South Korean government and a number of others have referred specifically to it and adopted bits of it. We have been very gratified to see that it has been very influential in that way.[182]

3.118 However, many submissions were concerned that, here in Australia, the Australian Government has thus far failed to respond to the report and that most of the report's recommendations have not yet been implemented.[183] For example, the NHMRC submitted that:

---

179 *Submission 12*, p. 6.

180 Productivity Commission, *Review of the Disability Discrimination Act* 1992, Inquiry Report No. 30, 20 April 2004, Volume 1, pp 300-301 and 304, Recommendation 11.1.

181 See, for example, NHMRC, *Submission 20*, p. 6; Cancer Council of NSW, *Submission 2*, p. 3; Centre for Law and Genetics, *Submission 24*, pp 5-7; Office of the Victorian Privacy Commissioner, *Submission 33*, p. 5; APF, *Submission 32*, p. 12; Anti-Discrimination Board of NSW, *Submission 12*, p. 8; LIV, *Submission 37*, p. 12; see also Ms Anna Johnston, APF, *Committee Hansard*, 19 May 2005, p. 19; Professor Don Chalmers and Dr Dianne Nicol, Centre for Law and Genetics, *Committee Hansard*, 20 May 2005, pp 8 and 11.

182 *Committee Hansard*, 19 May 2005, p. 44; see also ALRC, *Submission 18*, p. 1.

183 See, for example, AMA, *Submission 9*, p. 7; LIV, *Submission 37*, p. 12; NHMRC, *Submission 20*, p. 6.

> …implementation of the recommendations in *Essentially Yours* is important and should take place without further delay.[184]

3.119 The ALRC noted in its submission that:

> The Australian Government has not yet formally responded to the report, although it is understood that the Attorney-General's Department and the Department of Health and Ageing are coordinating a formal Whole-of-Government response.[185]

3.120 The Department of Health and Ageing submitted that the government is currently considering the report and is likely to provide a formal whole of government response.[186] Professor Weisbrot of the ALRC acknowledged that the ALRC report:

> …cuts across many portfolios, and I think that is the issue. It is being primarily coordinated by Health, and the Attorney-General's Department has been involved and active. But, looking at the subject matter here, my guess is that you would also have to deal with DIMIA, Workplace Relations, Education, Science and Technology, DFAT and, no doubt, a range of other departments. So I think it is probably a very large coordination project, and involves getting the sign off from all the various ministers and so on. I am not aware that there are any major issues of principle holding things up. I suspect it is more a question of the coordination. But again that is a third-party process impression.[187]

3.121 During the committee's hearing in Sydney, Professor David Weisbrot noted that he had heard informal reports that a response would be provided 'soon'. [188]

3.122 In response to the committee's questions on the issue, a representative of the Attorney-General's Department noted that 'the timing of the final release of government responses is of course a matter for ministers', and that:

> A considerable amount of work has been done and there are certain clearance processes that need to be gone through…there are a number of ministers and agencies that have some involvement in that. I cannot give you a specific date but a considerable amount of work has been done in putting together a response.[189]

3.123 Further, during the committee's hearings, Professor Weisbrot of the ALRC pointed out to the committee that, in the recent 2005-06 Budget:

---

184 *Submission 20*, p. 6.

185 *Submission 18*, p. 2.

186 *Submission 34*, p. 18; see also *Submission 34A*, p. 3.

187 *Committee Hansard*, 19 May 2005, p. 39.

188 *Committee Hansard*, 19 May 2005, p. 37.

189 *Committee Hansard*, 19 May 2005, p. 59.

> …the government allocated $7.6 million to establish a human genetics advisory committee. That would be another principal committee of the NHMRC. That basically implements the central recommendation of the ALRC's report, which is that we need a standing committee to monitor developments in this area and to provide expert advice—both technical scientific advice and advice about the ethical, legal and social implications of the new genetics.[190]

3.124 In response to the committee's questions, Professor Weisbrot noted that the ALRC's preference was for an independent, stand-alone commission because:

> …a commission would be likely to attract adequate resources, although I am reassured by the allocation that has been made now that it will have adequate resources to do the job; and, secondly, that not all the issues were purely health related.[191]

3.125 Professor Weisbrot stated that a committee of the NHMRC would be the ALRC's 'second preferred model', but that:

> …it should be a standards setting and advisory and coordination education body, rather than a regulator, and that the regulation function should go to other bodies that normally have that function.[192]

3.126 Professor Don Chalmers of the Centre for Law and Genetics also noted and described the budget proposal as 'a very good step forward'. He noted that although there are some matters which will not be fully classified as research or health, his understanding was that the NHMRC would have the capacity to deal with matters outside the health area.[193]

3.127 In response to the committee's questions on the issue, a representative of the NHMRC noted that:

> The committee has not yet been established but, as you say, it will be a principal committee of NHMRC, and it will be appointed by the minister following consultation with relevant stakeholders. It is anticipated that the principal committee will start its work to coincide with the beginning of the new triennium, which is January 2006.[194]

3.128 A representative of the Department of Health and Ageing explained to the committee:

> In the recent budget the government provided funds for the establishment of an expert advisory committee on human genetics. This will be established

190 *Committee Hansard*, 19 May 2005, pp 37-38.

191 *Committee Hansard*, 19 May 2005, pp 39-40.

192 *Committee Hansard*, 19 May 2005, pp 39-40.

193 *Committee Hansard*, 20 May 2005, p. 9.

194 *Committee Hansard*, 20 May 2005, p. 28.

> as a principal committee of the National Health and Medical Research Council. Its role will be to provide advice on current and emerging issues in human genetics and related technologies, and to provide advice on the complex social, legal, ethical and scientific issues that arise from these technologies. The reconciliation of the privacy of an individual with imperatives of research and the benefits that will give to individuals' families and communities will, of course, be among these current and emerging issues that it will advise on.[195]

3.129 In response to the Committee's requests for further details in relation to this proposed committee, the Department of Health and Ageing replied that the committee will be established from January 2006, and that the 'expertise and composition of the new committee are yet to be established.' The Department also noted that the new committee will work closely with the NHMRC and other Principal Committees, in consultation with the Minister.[196]

3.130 Some other aspects of the *Essentially Yours* report have also been implemented. For example, Professor Weisbrot noted that the *Family Law Regulations* had been amended in accordance with the ALRC's recommendations in relation to parentage testing:

> …the family law regulations were changed in accordance with the ALRC recommendations relatively recently…There was change to upgrade the identification and consent requirements in relation to laboratory testing for parentage purposes and that is what we did recommend in the report. So that has been done separately and did not require legislation; it was a new regulation. That was exactly in the terms that the ALRC recommended. So there are some improvements there.[197]

3.131 However, he noted that other aspects of the parentage testing recommendations had not yet been implemented, such as the proposal that only accredited labs do the testing.[198]

3.132 The Committee notes that the government has responded to the Productivity Commission's review of the *Disability Discrimination Act 1992*, and this response mentioned the ALRC and NHMRC's recommendations on genetic discrimination. The response stated:

> The Government accepts the concerns raised by the Productivity Commission and the [ALRC-NHMRC] Inquiry that the definition of disability needs to be clarified so that it includes a genetic predisposition to a disability. The current definition of disability includes disabilities that

---

195 *Committee Hansard*, 20 May 2005, pp 31-32.

196 *Submission 34A*, p. 3.

197 *Committee Hansard*, 19 May 2005, p. 40; see also ALRC, *ALRC 96 Implementation* at: http://www.alrc.gov.au/inquiries/title/alrc96/implementation.htm (accessed 31 May 2005).

198 *Committee Hansard*, 19 May 2005, pp 40-41.

> may exist in the future or are imputed to a person. The Government considers that this includes a genetic predisposition to disability. However, clarification is desirable to the extent that there is any doubt. The Government considers it would be more appropriate to provide an advisory note in the DDA [Disability Discrimination Act 1992], rather than amend the definition itself.[199]

Microchip implants and RFID technology

3.133 The Committee's terms of reference for this inquiry refer to microchips which can be implanted in human beings (for example, as recently authorised by the United States Food and Drug Administration).[200] The authorisation refers to the approval, in October 2004, by the United States Food and Drug Administration (US FDA) for the use of 'Verichip' technology for medical purposes.[201] The 'Verichip' is a miniaturised, implantable RFID. RFID has been described as:

> …tiny silicon chips that broadcast a unique identification code, when queried by a reader device using radio waves. At present, they can return such a signal from distances up to a few tens of metres depending on the communicating frequencies and transmitting powers involved. The tags may be as small as rice grains, positioned within ID cards, tokens, wristbands, or even under the skin, as in the use of microchips for pets.[202]

3.134 As the Office of the Victorian Privacy Commissioner observed:

> Although Radio Frequency Identification (RFID) was initially used primarily for tracking objects (such as individuals items of foodstuff, clothing and books), it is gradually being used to track people (such as children) by embedding RFID chips in clothing or cards.[203]

3.135 The 'Verichip', as approved by the US FDA, is described as 'a subdermal RFID device' about the size of a rice grain.[204] The manufacturer explains that each 'Verichip' contains:

> …a unique verification number that is captured by briefly passing a proprietary scanner over the VeriChip… A small amount of radio frequency

---

199 Attorney-General's Department, *Government's response to the Productivity Commission's Review of the Disability Discrimination Act 1992*, p. 8 at http://www.ag.gov.au/PCDDA (accessed 7 June 2005).

200 See term of reference (a)(ii)(D).

201 See, for example, L Dolinar, "Implantable chips in humans get the nod", *Sydney Morning Herald*, 15 October 2004, p. 11.

202 M James, "Where are you now? Location detection systems and personal privacy", *Parliament Library Research Note No. 60 2003-04*, 15 June 2004, p. 3.

203 *Submission 33A*, p. 2.

204 *FDA clears Verichip for medical applications in the United States*, http://www.4verichip.com/nws_10132004FDA.htm (accessed 1/02/2005).

> energy passes from the scanner energizing the dormant VeriChip, which then emits a radio frequency signal transmitting the verification number.[205]

3.136 The US FDA has approved the 'VeriChip' for medical uses – such as confirmation of identity, blood type, potential allergies and medical history of unconscious patients. However, according to the manufacturer, the 'VeriChip is not an FDA-regulated device with regard to other potential uses, such as security, financial, personal identification/safety applications'.[206] Indeed, the Office of the Victorian Privacy Commisioner noted that, according to Verichip, the technology is:

> …being actively developed for a variety of security, defense, homeland security and secure-access applications, such as authorized access control to government and private sector facilities, research laboratories, and sensitive transportation resources.[207]

3.137 Few submissions specifically addressed the issue of human microchip implants. Of those that did, several submissions suggested that the use of microchip implants should be prohibited, pending further research, public consultation and the implementation of a suitable regulatory regime.[208] For example, the NHMRC submitted that:

> If the use of implanted microchips involves tailoring the information to specific individuals as an extension of pharmacogenetics, for example full identification which could be useful in certain circumstances such as disaster victim identification, ethical issues including loss of freedom; compulsion or coercion of the individual to accept a microchip (especially minors); access to information contained on the microchip beyond health applications; and the individual's ability to update or change information as needed would arise. The NHMRC believes there needs to be a thorough and full examination of all the issues before such a proposal is considered further in Australia.[209]

3.138 Mr Roger Clarke expressed strong concern that proposals for the use of human microchips are 'coming forward in a regulatory vacuum', and in particular that:

---

205 *FDA clears Verichip for medical applications in the United States*, http://www.4verichip.com/nws_10132004FDA.htm (accessed 1/02/2005).

206 *FDA clears Verichip for medical applications in the United States*, http://www.4verichip.com/nws_10132004FDA.htm (accessed 1/02/2005).

207 *Submission 33A*, p. 3; see also http://www.4verichip.com/verichipfuture.htm (accessed 2 June 2005). Indeed, there are some reports of other uses overseas of microchips implanted in humans for security and other purposes: see further: B Feder and T Zeller, "Identity Badge Worn Under Skin Approved For Use in Health Care", *New York Times*, October 14 2004; see also Electronic Privacy Information Center, "Verichip", http://www.epic.org/privacy/rfid/verichip.html (accessed 1/2/2005).

208 Roger Clarke, *Submission 28*, p. 2; Caroline Chisholm Centre for Health Ethics, *Submission 10*, p. 10; NHMRC, *Submission 20*, p. 7.

209 *Submission 20,* p. 6.

> The much-heralded FDA 'approval' for chip-implantation was merely a statement that the procedure does not automatically violate health care laws.[210]

3.139 Mr Roger Clarke argued that:

> The Parliament has a responsibility to proscribe all uses of chips in or closely associated with humans, and to sustain the ban until after research and public consultation have been undertaken and a suitable regulatory regime devised and implemented.[211]

3.140 In response to the committee's questions on notice on this issue, the Office of the Victorian Privacy Commissioner expressed the view that implanting the RFA devices under the skin 'raises additional privacy concerns that need to be debated.' The Office noted the use of electronic monitoring has recently been authorised in Victorian law for serious sex offenders released from custody, but that the Victorian legislation 'is silent as to whether a tracking device can be implanted under the ex-offender's skin.'[212] The Office of the Victorian Privacy Commissioner argued that:

> Any such interference with bodily integrity, if ever contemplated in extraordinary circumstances, should only be done under clear authority of law or by voluntary and informed consent, and with appropriate safeguards to protect the health, privacy and dignity of the individual to be tracked, and those with whom he or she lives and associates.[213]

3.141 In contrast, other submitters commented on the possible benefits of such technology, depending on their application and use.[214]

3.142 The Department of Health and Ageing submitted that it was not considering the introduction of a microchip for human use here in Australia in the foreseeable future. However, the Department noted that such implants may not fall within the definition of 'therapeutic good' or 'medical device' under the *Therapeutic Goods Act 1989*, depending on the particular use and medical applications.[215]

3.143 In response to the Committee's questions on the issue of microchips, the Privacy Commissioner, Ms Karen Curtis replied:

> We have not provided any advice to any Australian government about microchips. One of the clear principles that underpin our Privacy Act is technology neutrality, so we would like to think that the Privacy Act would

---

210 *Submission 28*, p. 2.

211 *Submission 28*, p. 2.

212 *Submission 33A*, p. 3. The relevant legislation is the *Serious Sex Offenders Monitoring Act 2005 (Vic)*.

213 *Submission 33A*, pp 3-4.

214 Lockstep Consulting, *Submission 11*, p. 21; AEEMA, *Submission 26*, p. 2.

215 *Submission 34*, pp 19-20.

> be able to apply to some of these things. But in my report I am actually recommending that there be a wider review of the definition of personal information, because the principles are based on essentially 30-year-old notions.[216]

RFID technology

3.144 Some submissions raised concerns about the privacy implications of RFID technology at a broader level than its use in human implants.[217] For example, the Office of the Victorian Privacy Commissioner believed that:

> The use of RFID raises significant privacy issues around how it is used, when its use is justifiable, what other information is made accessible through the use of the device, and what safeguards apply to minimise the risk of misuse and provide redress.[218]

3.145 Similarly, the ACA described RFID devices as 'invisible bar codes', and was concerned that:

> RFID potentially brings all our possessions and purchases into the electronic realm, and thus has the potential to radically alter concepts and norms of ownership and personal information.[219]

3.146 The ACA did not suggest RFID-specific legislation, but submitted that:

> Many of the issues in RFID are challenges to existing and desirable generalist legislation. Many of the backend data accumulation issues should be covered in the Privacy Act, with appropriate treatment of what constitutes personal information. Other RFID issues are actually about surveillance and need attention in surveillance legislation, alongside optical and other techniques. It is this environment that would perhaps be best placed to deal with issues of implantable tags.[220]

3.147 It is noted that an international resolution on RFID has been adopted by data protection and privacy commissioners. The resolution calls for all the basic principles

---

216 *Committee Hansard*, 19 May 2005, p. 56.

217 See, for example, ACA, *Submission 15*, pp 4-5; EFA, *Submission 17*, pp 26-29; Caroline Chisholm Centre for Health Ethics, *Submission 21*, p. 6; Office of the Victorian Privacy Commissioner, *Submission* 33A, pp 2-4; also B Woodhead, "Electronic tags: are we next?", *Australian Financial Review*, 29 July 2003; M James, "Where are you now? Location detection systems and personal privacy", *Parliament Library Research Note No. 60 2003-04*, 15 June 2004, p. 3.

218 *Submission 33A*, p. 2.

219 *Submission 15*, p. 4.

220 *Submission 15*, pp 4-5.

of privacy law to be adopted when designing, implementing and using RFID technology.[221]

Other technologies and related issues

3.148 Submissions also raised a range of other technologies that it was suggested should be considered by this inquiry due to their privacy implications.[222]

3.149 For example, the AFP submitted that it was monitoring the emergence of 'Public Source Data' (PSD) companies in the US, although the extent of PSD activity in Australia is uncertain. The AFP explained that PSD companies focus solely on the collection of publicly available personal information from which detailed comprehensive personal profiles of individuals are compiled. These profiles are then sold to clients including credit agencies, private investigators and auditing companies. The AFP submitted that, while individual items of information obtained by PSDs may not breach current privacy legislation, the capacity of PSDs to aggregate such information and link it to high powered search engines provides a 'significant source of concern.'[223]

3.150 The ACA pointed to a number of technologies that it argued the Privacy Act had failed to adequately address, including: electronic messaging; video surveillance; location-based services; the integrated public number database, and 'spyware'.[224] In relation to 'spyware', it is noted that the Department of Communications, Information Technology and the Arts has released a discussion paper on the issue and has been conducting public consultation workshops around Australia.[225] Further, in March 2005, the Minister for Communications, Information Technology and the Arts released the outcome of a legislative review which concluded that 'spyware-related malicious activities are covered by existing laws', including the Privacy Act.[226]

3.151 Mr Roger Clarke also pointed to:

---

221 Office of the Federal Privacy Commissioner, *Media Release: World's Privacy Regulators call for privacy friendly RFID tags*, 9 December 2003, available at: http://www.privacy.gov.au/news/media/03_17.html (accessed 15 February 2005).

222 See, for example, ACA, *Submission 15*, pp 2-7; EFA, *Submission 17*, pp 7-19; Roger Clarke, *Submission 28*, p. 3; Lockstep Consulting, *Submission 11*, p. 1; LIV, *Submission 37*, p. 9.

223 *Submission 42*, p. 2; see also AFP, *Committee Hansard*, 20 May 2005, pp 39-40; and Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988*, March 2005, p. 240.

224 *Submission 15*, pp 2-7.

225 See further Department of Communications, Information Technology and the Arts, *Spyware,* http://www.dcita.gov.au/ie/spyware (accessed 31 May 2005).

226 Department of Communications, Information Technology and the Arts, *Outcome of the Review of the Legislative Framework on Spyware,* March 2005*;* See further http://www.dcita.gov.au/__data/assets/pdf_file/24939/Outcome_of_Review.pdf (accessed 31 May 2005).

> …a long list of additional technologies that should also be subjected to examination. Data mining, CCTV [closed circuit television], digital signatures, toll-roads that deny anonymous usage, pattern-recognition applied to car number-plates, caller-line identification, gross abuses of the 'white pages' database – IPND [Integrated Public Number Database], auto-identification of telephone callers, and location and tracking of mobile phones, have all demanded attention from public interest organisations. They should all be subjected to publicly funded policy research, and then to appropriate regulation in order to rein in the privacy abuses that they embody.[227]

3.152 The LIV suggested that other technologies to be considered could include:

> …digital cameras in mobile phones, GPS technology, light x-rays of airline passengers and video surveillance, and drug testing and fingerprinting of school children. Even more items could be added as new technologies, and new ways of applying existing technologies, are developed.[228]

3.153 The LIV also suggested that this inquiry should examine:

> …the individual systems that support these new technologies. This is particularly relevant to the LIV's submission as a breach of privacy may not occur at the 'front end' or 'user end' (ie where Smart Cards are being used), but rather at the 'backend' (ie at the server where all the information is stored). We suggest that attacks on the backend of these systems are common and may result in a breach of privacy.[229]

3.154 Electronic health records, and the Health*Connect* initiative, were also raised in several submissions.[230] These are considered further in chapter 5 of this report.

3.155 EFA raised concerns with other technologies, including telecommunications technology. For example, EFA was particularly concerned about the online surveillance of activities by internet users and other issues.[231] Indeed, EFA argued that:

> …individuals have almost no privacy 'rights' in the online environment and even the few privacy rights they allegedly have are not protected adequately and are difficult, sometimes impossible, to have enforced.[232]

3.156 EFA explained further

---

227 *Submission 28*, p. 3; see also see also Senate Select Committee on Information Technologies, *Cookie Monsters? Privacy in the Information Society*, November 2000.

228 *Submission 37*, p. 9.

229 *Submission 37*, p. 6.

230 See, for example, AMA, *Submission 9*; Department of Health and Ageing, *Submission 34*, pp 12 and 15; Ms Pamela Burton, AMA, *Committee Hansard*, 20 May 2005, p. 14.

231 *Submission 17*, pp 9-14.

232 *Submission 17*, p. 9.

> The lack of rights and/or adequate protection of rights arises from a combination of factors, including but not limited to, uncertainty regarding the definition of 'personal information'; no requirement to obtain consent before collecting personal information; use of bundled 'consents' including to disclose information to unspecified 'partners'; the small business exemption; and/or technological developments.[233]

3.157 Some of these issues, such as the bundled consent, are discussed further in relation to the private sector provisions in the next chapter of this report.

3.158 It is also noted that some of these other technologies are regulated by legislation other than the Privacy Act, such as telecommunications legislation. However, the inconsistency between the Privacy Act and telecommunications legislation was a problem for some submitters. For example, the APF and EFA suggested that there should be a review of the relationship between privacy and communications law.[234] This is also discussed in the next chapter of this report.

233 *Submission 17*, p. 9.

234 *Submission 32*, p. 9; see also EFA, *Submission 17*, esp. Appendix 1; ACA, *Submission 15*, p. 2.

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.

CHAPTER 5

OTHER ISSUES

5.1 This chapter examines some of the other issues raised during the inquiry. These include:

- the credit reporting provisions in Part IIIA of the Privacy Act;
- privacy in the health sector;
- the impact of the Privacy Act on medical research;
- the impact of the Privacy Act on responses to overseas emergencies;
- the impact of the Privacy Act on law enforcement issues;
- the use of the Privacy Act as a means to avoid accountability and responsibilities; and
- the impact of the Privacy Act on care leavers.

5.2 Each of these issues is considered below.

Consumer credit reporting

5.3 Part IIIA of the Privacy Act governs consumer credit reporting: that is, the handling of credit reports and other credit worthiness information about individuals by credit reporting agencies and credit providers.[1] The aim is to ensure that the use of this information is restricted to assessing applications for credit lodged with a credit provider and other legitimate activities involved with giving credit. Key requirements of Part IIIA include the following:

- Limits on the type of information which can be held on a person's credit information file by a credit reporting agency. There are also limits on how long the information can be held on file.
- Limits on who can obtain access to a person's credit file held by a credit reporting agency. Generally only credit providers may obtain access and only for specified purposes.
- Limits on the purposes for which a credit provider can use a credit report obtained from a credit reporting agency. These include:
  (a) to assess an application for consumer credit or commercial credit;
  (b) to assess whether to accept a person as guarantor for a loan applied for by someone else;
  (c) to collect overdue payments;
- A prohibition on disclosure by credit providers of credit worthiness information about an individual, including a credit report received from a credit reporting agency, except in specified circumstances.
- Rights of access and correction for individuals in relation to their own personal information contained in credit reports held by credit reporting agencies and credit providers.

---

1 This summary of Part IIIA and the Credit Reporting Code of Conduct is drawn from the OFPC website: http://www.privacy.gov.au/act/credit/index_print.html#key.

5.4 Part IIIA is supplemented by the Credit Reporting Code of Conduct issued by the Privacy Commissioner in accordance with the Privacy Act. The legally binding Code covers matters of detail not addressed by the Act. Among other things, it requires credit providers and credit reporting agencies to:

- deal promptly with individual requests for access and amendment of personal credit information;
- ensure that only permitted and accurate information is included in an individual's credit information file;
- keep adequate records in regard to any disclosure of personal credit information;
- adopt specific procedures in settling credit reporting disputes; and
- provide staff training on the requirements of the Privacy Act.

Concerns raised during this inquiry in respect of Part IIIA

5.5 Submissions raised significant concerns relating to the operation of Part IIIA of the Privacy Act.[2] These included the following.

Lack of consent to the use and disclosure of personal information

5.6 The Privacy Act is generally predicated on individuals' consent to the use and disclosure of their personal information.[3] Concerns were therefore raised over industry's use of 'bundled consents' whereby consent to disclose personal information to a credit reporting agency is 'bundled' into a group of other consents in credit or loan applications. Consumer advocates argue that the relevant forms and disclosure statements can be unreadable, confusing and appear designed not to invite consumers to read it.[4] Others argued that the market power of credit providers effectively negates any notion that a person is genuinely 'consenting' to how their personal information is to be handled. Refusal to sign bundled consents may mean that they cannot obtain housing or a telephone.[5] For these reasons, it was argued that reform is required to mandate standards for privacy and consent clauses.[6]

5.7 In contrast, industry maintained that any prohibition on secondary use of data or on bundled consent would be an unwarranted and intrusive restriction on business. As discussed in chapter 4, Baycorp Advantage argued that practices such as bundled

---

2 Legal Aid Queensland, *Submission 31*; Consumer Credit Legal Centre (NSW), *Submission 35*; CUSCAL, *Submission 36*; Consumers Federation of Australia, *Submission 40*; Baycorp Advantage, *Submission 43*; Australian Communication Exchange, *Submission 41*.

3 Paragraph 18E(8)(c) of the Privacy Act, for example, prevents credit providers from disclosing an individual's personal information to a credit reporting agency if the credit provider did not inform the individual before or at the time the information was acquired that the information might be disclosed to a credit reporting agency.

4 Consumer Credit Legal Centre (NSW), *Submission 35,* pp 14-15; Legal Aid Queensland, *Submission 31,* p. 8 of the Attachment.

5 APF, *Submission 32*, p. 4.

6 Consumer Credit Legal Centre (NSW), *Submission 35,* pp 14-16. See also the discussion in chapter 4 of this report on bundled consents.

consent create more efficient processes for business.[7] Baycorp Advantage also highlighted the importance of efficient credit reporting in managing exposure to financial risk by providing comprehensive data about the past credit behaviour of potential customers. For example:

> The production and provision of credit reports is in the public interest in a modern society which values the possibilities afforded by the easy availability of credit and the free flow of information. Moreover, the greater ability of businesses to assess and manage risk leads to the reduction of bad debt levels and to improved performance across the economy as a whole.[8]

Lack of procedural fairness and inaccurate records

5.8 Both industry and consumer advocates agree that credit reporting agencies' databases contain inaccurate data on consumers (although they differ on the extent to of this inaccuracy).[9] This is notwithstanding obligations imposed under Part IIIA for record keepers and credit reporting agencies to ensure that personal information contained in their records is accurate, up-to-date, complete and not misleading.[10] One reason for such requirements is that errors or inaccuracies can have a significant detrimental impact on individuals. As Legal Aid Queensland stated:

> Where the information in credit reporting databases is inaccurate, incomplete or misrepresents the facts, the ability of individuals to obtain credit is severely limited. In our experience, it can have the effect of forcing consumers into poverty or severe financial hardship … [and] cause severe emotional distress.[11]

5.9 Consumer advocates and representatives maintain that consumers are not informed of listings or inquiries made on their credit reports or even that they have a credit report. The fact that a credit report contains adverse information is generally only brought to consumers' attention when they are denied credit. This, it is argued, denies consumers the opportunity to check information held on them and to correct it.[12]

5.10 The committee was advised that credit reporting agencies – such as Baycorp Advantage – do provide a service whereby for a fee they will notify consumers if

---

7 Baycorp Advantage, *Submission 43*, pp 3 and 14.

8 *Submission 43*, pp 7-8.

9 See, for example, the figures cited in Consumer Credit Legal Centre (NSW), *Submission 35,* pp 5-6; Kirsty Needham, 'Bad debt files purged after privacy watchdog's finding', *Sydney Morning Herald,* 27 August 2004, p. 4; Baycorp Advantage, *Submission 43*, pp 8-9.

10 Section 18G of the Privacy Act requires credit reporting agencies to take reasonable steps to ensure that personal information contained in credit file or report is accurate, up-to-date, complete and not misleading. Privacy Principles also require record keepers not to use information without first taking steps to ensure that this is accurate.

11 Ms Lorretta Kreet, Solicitor, Legal Aid Queensland, *Committee Hansard*, 22 April 2005, p. 25.

12 Catherine Wolthuizen, 'Reporting on the credit reporters', *Consuming Interest*, Autumn 2004, p. 7.

alterations are made to their credit reports.[13] The committee also understands that consumers are able obtain a copy of their credit report free of charge from credit providers such as BayCorp Advantage. However, it is also generally acknowledged that individuals are not utilising these services or taking an active interest in the management of their credit records. As Baycorp Advantage stated, 'until there is a problem, consumers typically do not look'.[14]

5.11 Consumer advocates maintain that a disincentive for consumers is the difficulties they can face in trying to correct inaccurate information held by credit reporting agencies.[15] It is argued that such difficulties stems in part from poor drafting and ambiguous provisions.[16] The lack of an effective complaint handling system is cited as another reason. Critics argue that there is no real requirement for entities such as credit providers to establish internal dispute resolution procedures for those consumers who wish to correct their records. Moreover, the dispute resolution procedures that are established by credit providers and/or credit reporting agencies lack transparency and fail to address complaints in relation to repeated problems or possible systemic issues.[17] Concerns were also raised that dispute resolution procedures generally place the onus of proving that listings are inaccurate on individual consumers who lack any real bargaining power. As the Consumer Credit Legal Centre stated:

> … [it] relies on consumers having knowledge of the credit reporting agency, knowing how to access their individual report, accessing their individual report and making a complaint if unauthorised access or incorrect details are contained in the report. In most cases, the first time an individual [may become aware of or] may seek access to their credit report is when

13 Some suggest that the costs of such a service can act as a disincentive given the number of entities involved. See Legal Aid Queensland, *Submission 31*, p. 2.

14 Mr Andrew Want, Baycorp Advantage Pty Ltd, *Committee Hansard*, Thursday, 19 May 2005, p. 2.

15 This is notwithstanding section 18J of the Privacy Act which, for example, states that credit reporting agencies must make appropriate corrections, deletions and addition to ensure that the personal information contained in the file or report is accurate, up-to-date, complete and not misleading.

16 Consumer Credit Legal Centre (NSW), *Submission 35,* p. 5. See also Legal Aid Queensland, *Submission 31,* pp 2-4. For example, IPP 8 requires record keepers not to 'use' information without first ensuring accuracy. However, it is suggested this does not prevent credit reporting agencies from accepting as opposed to using inaccurate information or records. Similarly, statutory requirements that credit reporting agencies 'take reasonable steps' to ensure accuracy of information they are provided with beg the question of what they can 'reasonably' do given the high volume of information that they handle. Baycorp's credit reporting databases hold 14 million credit reports and personal information on almost 90 per cent of the adult population of Australia. See Baycorp Advantage, *Submission 43*, p. 3; Mr Andrew Want, Baycorp Advantage, *Committee Hansard*, Thursday, 19 May 2005, p. 5.

17 Consumer Credit Legal Centre (NSW), *Submission 35,* pp 18-19. See also Legal Aid Queensland, *Submission 31*, p. 3.

> credit is refused on the grounds of an adverse credit report and or where the individual in threatened with a default listing.[18]

5.12 It would appear that the OPC as regulator can be of little assistance in this regard. The committee received evidence from both industry and consumer organisations indicating that the OPC is currently ill-equipped to respond to consumer complaints. Consumer advocates claim that the OPC's complaints handling process is inconsistent, inefficient and lacks transparency and procedural fairness, with the result that large numbers of individuals drop out of the system.[19] As explained elsewhere in this report, it can take six months or more before complaints can be heard by the OPC, and affected individuals may be unable to access credit during this period.[20] The OPC's ability to enforce the Act in cases of proven non-compliance is also questioned.[21] Baycorp Advantage confirmed that resourcing issues had led the OFPC to ask it to try to resolve consumer complaints in the first instance.[22] Critics argue that this in turn has prompted confusion over responsibility for resolution of complaints. As the Consumer Credit Legal Centre explained:

> … a complaint is required to be made in writing 3 or 4 times, to Baycorp, then the OFPC, then the credit provider, then back to the OFPC. The OFPC requires written proof of complaint to the credit provider before the OFPC would investigate.[23]

5.13 Consumer concerns over the lack of a clear path for complaints resolution have been recognised by Baycorp, which is seeking to develop better dispute resolution mechanisms. It advised the committee that it is currently considering the establishment of an external dispute resolution mechanism in addition to its own internal processes and consumer recourse to the Privacy Commissioner.[24] It explained that:

> … this is an area in which we are engaging heavily with our subscriber customers [ie, credit providers] — both to define clear responsibilities within our subscriber organisations for dispute resolutions raised by

---

18 Consumer Credit Legal Centre (NSW), *Submission 35,* p. 2. See also Australian Privacy Foundation, *Submission 32*, p. 3.

19 Consumer Credit Legal Centre (NSW), *Submission 35,* pp 18-19. Legal Aid Queensland, *Submission 32*, p. 5. It is alleged that the OPC's complaints handling procedures deny consumers procedural fairness in that the OPC undertakes partial investigations of matters and then can decline to continue the investigation: that is, without consideration of all the evidence and without a final determination.

20 Consumer Credit Legal Centre (NSW), *Submission 35,* pp 18-19.

21 Consumer groups, for example, cite advice from the OPC that, while it has the power to audit credit reporting agencies, it cannot force compliance where breaches of the Act are identified and that resources are insufficient to allow further audits to be taken. See, for example, Catherine Wolthuizen, 'Reporting on the credit reporters', *Consuming Interest*, Autumn 2004, p. 7.

22 Mr Andrew Want, Baycorp Advantage Pty Ltd, *Committee Hansard*, Thursday, 19 May 2005, p. 5.

23 Consumer Credit Legal Centre (NSW), *Submission 35,* p. 19.

24 Baycorp Advantage, *Submission 43*, p. 10.

> consumers and to provide an alternative dispute resolution mechanism that consumers can have access to speed up the process of resolution.[25]

5.14 Notwithstanding such developments, concerns remain that compliance with privacy laws and requirements will not be a priority for industry without the incentives provided by effective regulatory oversight. Consumer advocates and representatives argue that, unless the OPC is provided with greater resources to take enforcement action and then prioritise enforcement action, the legislation will remain ineffective.[26] Baycorp Advantage also agreed that 'overall effectiveness could be improved by the provision of additional resources to the Office of the Federal Privacy Commissioner, in particular to assist with complaint handling'.[27]

Increasing access to credit reporting

5.15 Concerns were raised that the problems outlined above have been compounded by the proliferation in entities accessing the credit reporting system. Determinations issued by the Privacy Commissioner under Part IIIA of the Privacy Act have extended access to the credit reporting system beyond traditional lenders such as banks to a wide range of retailers and service providers. Video store operators, legal services and healthcare providers, for example, are now deemed to be credit providers.[28] Part IIIA also allows consumers to be listed with credit reporting agencies for old and/or small debts (which some argue are irrelevant to any assessment of default risk). Consumer advocates maintain that such broad access and the ability to list small or old debts increases the number of listings being made with credit reporting agencies and, therefore, the capacity for errors if effective mechanisms are not in place to ensure details are accurate and up-to-date.[29]

5.16 Consumer advocates also maintain that such broad access has made the credit reporting system vulnerable to abuse. Legal Aid Queensland, for example, advised the committee that:

> … [t]he use of credit reporting as a means for extracting payment for a disputed debt is rife. … The single biggest issue that has arisen over the past few years is … the threat of default listing or listing an individual as a

25 Mr Andrew Want, Baycorp Advantage Pty Ltd, *Committee Hansard*, Thursday, 19 May 2005, pp 3, 5.

26 Legal Aid Queensland, *Submission 31*, p. 2.

27 Baycorp Advantage, *Submission 43*, p. 3.

28 Copies of the relevant determinations are available on the OPC website at: http://www.privacy.gov.au/act/credit/deter1_02.html. It is suggested that access to credit reporting has now gone well beyond what was originally intended by those who enacted the legislation and who had sought to ensure access to credit reporting was very restricted. See Legal Aid Queensland, *Submission 31*, p. 2 of the Attachment.

29 See, for example, Catherine Wolthuizen, 'Reporting on the credit reporters', *Consuming Interest*, Autumn 2004, p. 7. See also Legal Aid Queensland, *Submission 31*, pp 2-4 of the Attachment.

means of forcing individuals to make payments on accounts where there is a dispute as to liability.[30]

5.17 The committee also received evidence suggesting that it is increasingly common for consumers to be denied credit on the basis of the number of inquiries made on their credit report, despite them having no adverse listing.[31]

Calls for reform

5.18 The concerns outlined above have prompted calls for a review of the credit reporting system, and particularly Part IIIA of the Privacy Act.[32] Reform proposals put forward by consumer groups have included the following:

- that only debts of $500 or more may be listed;
- that listing companies be required to demonstrate the existence of the debt and failure to pay;
- that consumers be notified when adverse listings, such as defaults and clearouts, are added to their file;
- that disputed debts be prevented from being listed while the dispute is being resolved;
- that an industry-funded external dispute resolution scheme be established, similar to those operating in the financial sector and approved by the Australian Securities and Investment Commission under the *Financial Services Reform Act 2001* (Cth); and
- that credit providers only be allowed access upon demonstration of satisfactory internal dispute resolution procedures and membership of the external dispute resolution scheme.[33]

5.19 In light of the above, submitters were critical of the federal government's decision to exclude the credit reporting provisions from the OPC review of the private sector provisions of the Privacy Act.[34]

30 Legal Aid Queensland, *Submission 31*, pp 7- 8. The Consumer Credit Legal Centre also cited instances where a default may be listed on a person's credit report despite the fact that they have disputed and are in fact still disputing liability for the debt. This, it is suggested, has the effect of coercing consumers to pay off the debt even though they may not be liable for it in order to have the listing removed and apply for credit. See Consumer Credit Legal Centre (NSW), *Submission 35,* pp 4, 8.

31 See, for example, *Submission 35,* p. 10.

32 See Legal Aid Queensland, *Submission 31*; Consumer Credit Legal Centre (NSW), *Submission 35*; Consumers Federation of Australia, *Submission 40*.

33 See, for example, Legal Aid Queensland, *Submission* 31, pp 6-9; Consumer Credit Legal Centre (NSW), *Submission 35.* See also: Catherine Wolthuizen, 'Reporting on the credit reporters', *Consuming Interest*, Autumn 2004, pp 7-8; Gabrielle Curtis, 'Consumer Watchdog calls for reform of credit blacklists', *The Age*, Saturday 8 May 2004, p. 7.

5.20 Industry representatives appear less sanguine about the need for a review or legislative reform. Baycorp Advantage advised the committee that, in its view, any formal review of Part IIIA or the related Code at this stage would impede the progress of measures underway to enhance effectiveness of the Privacy Act. As mentioned above, these measures include initiatives to enhance data quality and to improve consumer engagement, including the development of better dispute resolution mechanisms. An apparent concern for industry was that any proposals to further amend the privacy legislation had to be very carefully weighed against the accompanying compliance costs that legislative and regulatory change can cause, and which are ultimately borne by consumers.[35] Also highlighted was the credit reporting regime's important role in facilitating risk management (described above).

Positive reporting

5.21 The economic benefits of credit reporting were also cited in support of arguments that Part IIIA of the Privacy Act should be amended to permit positive credit reporting**.** The Privacy Act generally limits the range of personal information that can be contained in a credit report or file to 'negative' data, such as previous credit applications, defaults and credit infringements.[36] Submissions received by the committee indicated some debate on whether these restrictions should be removed in order to allow positive credit reporting. Positive credit reporting (also known as open file or comprehensive credit reporting) involves a much broader range of consumers' personal financial information being obtained and recorded by credit reporting agencies.[37]

5.22 Industry submissions stressed the economic advantages for Australia of moving to positive credit reporting. The current restricted regime, it is suggested, hinders credit providers from making fully informed decisions about credit applications. Positive credit reporting would enable a more accurate risk assessment

---

34 See, for example, Consumer Credit Legal Centre (NSW), *Submission 35,* p.3. See also OPC, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988*, March 2005, p. 23. This exclusion was despite earlier media reports that the Commonwealth Attorney-General's Office had stated that a review of the credit reporting system would be undertaken. See *The Age*, Saturday, 8 May 2004, p. 7. The Commissioner's report states that the credit reporting provisions were considered where relevant to the operation of the private sector provisions. Her report at page 267 acknowledges the concerns raised by consumer representatives that adequate systems are not in place to ensure data quality of credit report listings.

35 Baycorp Advantage, *Submission 43*, pp 3, 6, 8. Credit Union Services Corporation, *Submission 36*, p.1.

36 See section 18E of the Privacy Act. [Credit reports' contents are generally restricted to: personal details (name, address, employment, date of birth and driver's licence); previous credit applications; overdue payments (defaults) and serious credit infringements (such as non-payment of debts); bankruptcies; court orders; and public information (such as directorships).]

37 For example, information concerning the balance of credit accounts, amount of collateral and payment patterns.

and will thereby benefit both credit providers and consumers. As Baycorp Advantage stated:

> It is fairly clear that comprehensive reporting improves the quality of credit decisions, improves the efficiency of the credit information system as a whole. … It gives consumers the ability to manage their credit history in the most positive way, and that gives them the ability to shop for the best deals and really get the best out of the competitive environment that has been created in consumer lending. For business, there is a clear improvement to the quality of the credit books, and that is a benefit to the economy. There is a benefit to society generally through improved efficiency in the allocation of credit across the economy.[38]

The committee notes that these appear no different to industry claims made when the privacy provisions were first enacted.

5.23 In contrast, consumer advocates and representatives argue against any extension of Australia's current credit reporting regime. They question research cited by industry in support of positive credit reporting, pointing to other research and overseas experiences suggesting that there is no correlation between positive credit reporting and reduced levels of over indebtedness. Also questioned is the need for positive reporting in the Australian context given low default levels, current lending practices, the information currently available to credit providers and the fact that not all of this available information is used by credit providers.[39]

5.24 Baycorp Advantage advised the committee that, while it supported the introduction of positive credit reporting, it believed that there needs to be agreement with consumer groups that real progress has been made to improve the consistency and accuracy of data used for personal credit ratings and access to dispute resolution.[40] The committee also notes that there appears to be mixed views within industry on any move towards positive credit reporting. As the Chief Executive of the Australian Banking Association reportedly stated that:

> The issues surrounding positive reporting are complex and there are stakeholder concerns which must be considered. The ABA's [Australian Banking Association's] position is [that] there needs to be more information in the public domain to support an informed public debate about the

38 Mr Andrew Want, Baycorp Advantage Pty Ltd, *Committee Hansard*, Thursday, 19 May 2005, pp 3-4. See also Credit Union Services Corporation (Australia) Ltd, *Submission 36*, p 2.

39 Consumer Credit Legal Centre (NSW), *Submission 35,* pp 11-14 See also Catherine Wolthuizen, 'Open Sesame!', *Consuming Interest*, Spring 2004, pp 15 -17. Catherine Wolthuizen, Australian Consumers Association, 'Self-interest gags credit reporting' *Australian Financial Review* 18 February 2005. Joyce Moullais, 'Baycorp baulks at credit check reforms', *Australian Financial Review*, 26 April 2005, p. 55.

40 Mr Andrew Want, Baycorp Advantage Pty Ltd, *Committee Hansard*, Thursday, 19 May 2005, p. 3

> benefits and disadvantages of positive credit reporting. This is essential to the development of sound policy.[41]

5.25 The committee notes that experience with the current range of information has shown that industry has not run the system as well as would be expected and it is apparent that injustice can prevail. As well, positive reporting is also rejected on the basis that it would magnify the problems associated the accuracy and integrity of the current credit reporting system.[42] The privacy and security risks associated with the existence of large private sector databases containing detailed information on millions of people are of major concern.

Health information

Privacy protection - integral to health care

5.26 The importance of privacy in the provision of health care cannot be understated. As the Department of Health and Ageing stated:

> Privacy is a fundamental principle underpinning quality health care. Without an assurance that personal health information will remain private, people may not seek the health care they need which may in turn increase the risks to their own health and the health of others. Indeed consumers regard health information as different to other types of information and consider it to be deeply personal.[43]

5.27 This is borne out by the OPC's research on community attitudes towards privacy, confirming the importance that individual Australians place on the protection of their health information.[44] It is also demonstrated by the possible consequences for Australians when their health information is inadequately protected. As the OPC recently acknowledged:

> There are risks of serious harm arising from a failure to adequately protect an individual's health information, for example when handling genetic information that indicates an individual's susceptibility to a serious disease or information about an individual's sexual health. Some individuals may be stigmatised or discriminated against if their health information is mishandled.[45]

5.28 In light of the above, most, if not all, Australians recognise that a strong and effective privacy framework is required to regulate how and when an individual's health information may be collected, stored and disclosed to others.[46]

---

41 Joyce Moullais, 'Baycorp baulks at credit check reforms', *Australian Financial Review*, 26 April 2005, p. 55. See also Marc Moncrief, 'Debt experts clash over credit files', *The Age*, 11 April 2005, p. 3

42 See sources at footnote 39.

43 Department of Health and Ageing, *Submission 34*, Attachment, p. 3.

44 OPC review, p. 64.

45 OPC review, p. 64.

46 See, for example, Department of Health and Ageing, *Submission 34*, Attachment, p. 4.

5.29 However, evidence presented to the committee suggests that the privacy protection provided for health information in Australia – including that offered by the Privacy Act - is neither strong nor effective.

Overlapping, incomplete and inconsistent regulation

5.30 At present, the privacy of Australian's health information is protected by a patchwork of public and private sector legislation, common law and codes of conduct. These are outlined below.

Federal laws

5.31 The Privacy Act regulates the handling of health information by the private sector and by Commonwealth and ACT government agencies. The Act requires personal 'health information' to be afforded the highest privacy protection available, given the above-mentioned importance of such information and the sensitivity surrounding its collection and use.[47] This is also recognised by the fact that the Act's requirements apply to all private sector organisations that both hold health information and provide health services[48], regardless of annual turnover. As previously explained, a private sector organisation covered by the Act generally must not do anything that breaches an approved code binding on it. If not bound by an approved code, it must not do anything that breaches an NPP.[49]

5.32 For their part, Commonwealth and ACT government officials must comply with the IPPs as well as a range of other laws governing the disclosure of personal information by public sector agencies. Officers working in the federal health portfolio

---

47 'Health' information is defined by section 6 of the Privacy Act as:

(a) information or an opinion about: (i) the health or a disability (at any time) of an individual; or (ii) an individual's expressed wishes about the future provision of health services to him or her; or (iii) a health service provided, or to be provided, to an individual; that is also personal information; or

(b) other personal information collected to provide, or in providing, a health service; or

(c) other personal information about an individual collected in connection with the donation, or intended donation, by the individual of his or her body parts, organs or body substances.

The same section defines 'health information' as a specific type of personal information - 'sensitive information about an individual'. The latter requires a more rigorous protection under that Act. For example, NPP 10 imposes restrictions on whether and how an organisation can collect health information about an individual and NPP 2 imposes stricter limits on how sensitive information may be used or disclosed than is the case for non-sensitive personal information. See Centre for Law and Genetics, *Submission 24*, p. 5.

48 The Privacy Act stipulates providing a 'health service' includes any activity that involves: assessing, recording, maintaining or improving a person's health; or diagnosing or treating a person's illness or disability; or dispensing a prescription drug or medicinal preparation by a pharmacist. Health services therefore covered include traditional health service providers such as private hospitals and day surgeries, medical practitioners, pharmacists, and allied health professionals, as well as complementary therapists, gyms, weight loss clinics and many others. See OPC, Health Information and the *Privacy Act 1988* - A short guide for the private health sector. December 2001. Copy available at http://www.privacy.gov.au/publications/hp.html.

49 OPC review, pp 29-30.

must consider the IPPs in conjunction with, for example, the secrecy provisions of the relevant public service, health and aged care legislation.[50]

State and territory privacy regimes

5.33 State and territory governments have implemented their own arrangements to ensure the privacy of health information. Some have enacted privacy legislation governing their public sectors' use of such information. Others have administrative arrangements for this purpose. For example, Queensland has established two administrative standards for privacy in its public sector (one scheme for health sector agencies, and one scheme for other government agencies). State governments have also enacted laws regulating the handling of health information in the private sector. Victoria, for example, has enacted the *Health Records Act 2001* which aims to cover both the public and private sectors in that state and which is similar to the NPP provisions of the Privacy Act. New South Wales has similar legislation in place in the form of the *Health Records and Information Records Privacy Act 2002*.[51]

5.34 Federal privacy laws prevail over the state or territory privacy legislation, to the extent that these laws are inconsistent.

Industry, professional and common law privacy obligations

5.35 In addition, those involved in the provision of health care are bound by privacy obligations arising out of their common law confidentiality duties involved in the provider-patient relationship, as well as ethical and professional obligations (such as those imposed by codes of practice and professional service charters).[52]

Complexity and confusion for officials, heath care providers and patients

5.36 The result of the above-mentioned patchwork of legislation, common law and codes of conduct appears to be considerable confusion and undue complexity.

5.37 Differences exist in protection or coverage. Health information is subject to different protections depending on whether it is held by a federal agency, state or territory agency or private sector agency. Adding to this complexity are the different requirements that also apply to the information held by any one agency. As noted above, the Privacy Act itself imposes different requirements depending on whether the information held is personal information, health information and other sensitive information. Differences between jurisdictions compound the problem. As the OPC noted, 'each jurisdiction's scheme is slightly different, as are the principles on which they are based'.[53] Health information may also subject to different protections

50 OPC review, pp 64-5. Department of Health and Ageing, *Submission 34*, Attachment, pp 6-7.

51 OPC review, pp 64-5. Department of Health and Ageing, *Submission 34*, Attachment, pp 6-7

52 OPC review, pp 64-5. Department of Health and Ageing, *Submission 34*, Attachment, pp 6-7 Caroline Chisholm Centre for Health Ethics, *Submission 21,* pp 2-3.

53 OPC review, p. 64. See also Professor Colin Thomson, *The Regulation of Health Information Privacy in Australia. A description and comment*, (National Health and Medical Research Council Privacy Committee, Commonwealth of Australia, January 2004).

depending on which jurisdiction it is being held, collected or used in. As the Anti-Discrimination Board of New South Wales stated:

> A complicating factor is that many different organisations may be responsible for delivery of health services to any one individual meaning that different legal regimes and privacy protection, with differing standards apply to different parts of the health information relating to a single individual. Practical difficulties can also arise when organisations are required to comply with a number of related but conflicting laws – especially if States and Territory have health privacy legislation purporting to cover the private sector (NSW, Victoria and the ACT).[54]

5.38 Others argue that the fragmented nature of privacy protection has left significant gaps in coverage, with, for example, state government agencies and universities falling outside the scope of the federal legislation.[55] In this regard, the absence of national standards governing the secure storage and transmission of electronic health information was also criticised. The AMA argued that this is an issue than can only be addressed at the federal level:

> Stronger provisions and greater resources at the Federal level are required to properly address the security of electronic health records, and to prevent corporate misconduct for the on selling of health data. The push to make profits in GPs' practices bought by corporate interests raises the risk of inappropriate 'data-mining' of personal data for commercial purposes.[56]

5.39 Differences in protection or coverage also create significant compliance costs, particularly for those health care providers which operate in more than one jurisdiction. The OPC, for example, cited the instance of a national medication service operating via a call centre that had to read different statements to obtain consent depending on the location of the individual (and the law that applies in that jurisdiction).[57]

5.40 It is argued that the problems of inconsistency, complexity and fragmentation are getting worse as states and territories increasingly introduce their own privacy legislation.[58]

5.41 In view of the above, deciphering who has what rights in respect of what health information about which individual can be challenging. As the AMA stated:

> It is very difficult for medical practitioners and organisations that handle health information to comply with the public/private, Federal/State

54 Anti-Discrimination Board of New South Wales, *Submission 12*, p. 5.

55 Centre for Law and Genetics, *Submission 24*, p. 4.

56 Australian Medical Association, *Submission 9*, pp 2, 10.

57 OPC review, p. 66.

58 See OPC review, p. 42. See also Centre for Law and Genetics, *Submission 24*, p. 4. Tasmania, for example, has enacted personal privacy laws which have yet to commence. Professor Chalmers and Dr Dianne Nicol, *Committee Hansard*, 20 May 2005, p. 9.

> mishmash of regulation. This is being made more complex by emerging technologies.[59]

5.42 The LIV also highlighted the significant difficulties that many health providers face in trying to manage health information in a way that respects their patient's privacy and confidentiality:

> There is a significant degree of confusion surrounding the operation of the Privacy Act and other privacy laws in the health sector. … Recent cases [brought against health care providers] demonstrate the lack of understanding of fundamental privacy concepts and principles within the health sector … . We suggest that this confusion does not arise solely from a misunderstanding by health professionals of the Privacy Act. Rather, it is exacerbated by the variation between federal, state and territory legislation. Such legislation is broader than the Privacy Act and includes the various freedom of information, state privacy and other health legislation.[60]

5.43 The APF was particularly critical of the 'proliferation of health specific privacy rules and laws.' The Foundation argued:

> The confused situation that many health service providers currently find themselves in – being covered by at least two separate health privacy laws - federal and State or Territory – represents a failure of good government and is definitely not in the interests of consumers.[61]

5.44 The Department of Health and Ageing agreed that the complex arrangements outlined above are confusing for consumers who are unsure which legislation applies under what circumstances.[62] This confusion can undermine the enforcements mechanisms contained within the Privacy Act, which some argue are already 'relatively weak'. As the Centre for Law and Genetics noted:

> The federal privacy regime is complaints-driven and conciliation-based. In the first instance, health consumers have to be aware of their rights to be in a position to understand that they can bring a complaint under the legislation. The rights of aggrieved individuals are [already] limited under the existing legislation because in the event that orders are made by the Privacy Commissioner, such orders can only be enforced by court action.[63]

---

59 Australian Medical Association, *Submission 9*, p. 3.

60 Law Institute of Victoria, *Submission 37*, p. 7.

61 Australian Privacy Foundation, *Submission 32*, pp 8-9. Submissions received by the OPC during its review of the private sector provisions of the Privacy Act also 'overwhelmingly supported the conclusion that the existing state of health privacy laws in Australia is unsatisfactory for health service providers and individuals'. OPC review, pp 64, 68.

62 Department of Health and Ageing, *Submission 34*, p. 14 and Attachment, p. 8. The Department provided one example of the effect of several layers of privacy regulation. In giving advice to ACT pathologists who were changing their forms in a way that gave rise to privacy implications, the Department had to refer to the Privacy Act (the IPPs and NPPs), the *Health Records (Privacy and Access) Act 1997 (ACT)* and other ACT legislation, applying to pathologists operating as a private sector organisation. Department of Health and Ageing, *Submission 34*, p. 14 and Attachment, p. 8. See also OPC review, p. 40.

63 Centre for Law and Genetics, *Submission 24,* p. 4. See also the sections of this report concerning the resourcing of and enforcement by the OPC.

5.45 Conversely, the differing arrangements between jurisdictions can also lead to forum shopping, with potential plaintiffs shopping around to select the most suitable legislation to further their cause or grievance.[64]

5.46 It appears somewhat of a paradox that the various competing privacy laws, common law duties and codes of conduct that give rise to the above-mentioned problems all share the same objective; that is 'to regulate the handling of sensitive information, and to ensure its protection.'[65] Also incongruous is that the Privacy Act's private sector provisions – which had the objective of establishing a single comprehensive national scheme (provided through codes adopted by private sector organisations and the NPPs) – appear to have merely added to the problem. As the Department of Health and Ageing advised:

> [I]t is our experience that the private sector provisions now form just one of several layers of privacy requirements and legislation applying to the health sector, thus contributing to the complexity faced by both public and private sectors when addressing health privacy issues.[66]

Impediment to national health initiatives

5.47 Submissions and witnesses argued that the patchwork of laws, regulations and rules of conduct governing the handling of health information privacy in Australia also present a barrier to much needed reform. For example, the lack of consistent national health privacy laws have been cited an impediment to efforts to establish a national health information network.

5.48 Federal, state and territory Governments are implementing a national health information network known as Health*Connect*.[67] Health*Connec*t is a cooperative venture between the federal, state and territory governments to develop a national network of linked databases containing patient health records. It will provide for the electronic collection, storage and exchange of clinical information among health care providers.[68] Information recorded in Health*Connect* about an individual may be downloaded by health service providers, subject to the individual's consent, wherever and however they encounter health services across Australia. The aim is to integrate and better coordinate the flow of information across the different parts of the health sector (such as hospitals, general practitioners, specialist surgeries, pharmacies, pathology laboratories, etc) and thereby improve patient treatment.

---

64 OPC review, p. 67.

65 OPC review, p. 64.

66 Department of Health and Ageing, *Submission 34*, Attachment, p. 5.

67 The summary provided is taken from Department of Health and Ageing, *Submission 34*, pp 10-12 and Attachment, pp 14-15. See also http://www.healthconnect.gov.au/about/index.htm and http://www.ahic.org.au/strategy/index.html.

68 Implementation of Health*Connect* has begun in Tasmania, South Australia and the Katherine region of the Northern Territory, while discussions and other projects are underway in New South Wales, Queensland, Victoria, Western Australia and the ACT.

5.49 Related initiatives are the development of the Medicare smartcard and an individual national health identifier. The Medicare smartcard is intended to ensure the accurate and safe identification of people participating in clinical e-health schemes. As discussed in chapter 3, the Smartcard will hold a consumer identifier or national health identifier for e-health initiatives such as Health*Connect*. The Department of Health and Ageing explained the need to develop an identifier for each Australian as follows:

> To fully harness the benefits of new information technologies in the health care sector, it is critical that the means are in place to ensure that the electronic exchange of clinical information is accurately and securely matched to the right individual. Failure to do so could result in clinical decision making being compromised. In this context, there has been growing recognition that a unique patient identifier is needed across the health sector as a key building block for the national e-health agenda.[69]

Possible risks to privacy

5.50 It is clear that e-health initiatives and technological change can offer significant benefits in the heath care sector and improve patient care. Yet at the same time they create significant potential risks. As the AMA explained:

> New technology permits access to a wide range of information that can contribute to improvements in the delivery of healthcare and health outcomes for patients. The ultimate development of a national electronic health record has the potential to provide the means to share an individual's health information for the purposes of their health care needs throughout their lifetime. Access to a reliable, historical record of an individuals' encounters with the health system throughout their lifetime can contribute to safety and quality in the delivery of health care, particularly as the patient moves in and out of different parts of the health system. However, such systems also provide a source of data on individuals that has never before been available in a form that can be interrogated and linked so easily and so widely. This new environment, while creating the potential for significant positives in improving health care, has at the same time created significant potential risks to the privacy of individual health information and the independence of a medical practitioners' clinical decision making.[70]

5.51 A range of privacy concerns have been raised with respect to e-health initiatives such as the initiatives outlined above. These include concerns over access to and use of electronic health information data for secondary, unrelated purposes, the accuracy and security of collected data, and the risk of function creep.[71] As the AMA noted, such concerns impact on confidence in, and acceptability of, the proposed electronic systems for both patients and providers.[72]

---

69 Department of Health and Ageing, *Submission 34*, p. 10.

70 Australian Medical Association, *Submission 9*, p. 5.

71 See, for example, chapter 3 of this report which canvasses concerns surrounding the Medicare smartcard. See also Moira Paterson, 'Developing privacy issues in the growing area of health IT', *Australian Health Law Bulletin*, Vol.13, No. 8, May 2005, pp 89 – 95.

72 Australian Medical Association, *Submission 9*, p. 5.

Need for new privacy rules

5.52 It is recognised that privacy protection will be a critical component of Health*Connect* and the related initiatives outlined above. That is, 'ensuring the privacy, confidentiality and security of personal health information would be paramount to both consumer and health provider acceptance of such initiatives'.[73] Yet it was equally clear that, for the reasons outlined above, existing health specific privacy rules and laws cannot be relied upon to ensure acceptance. As the Department of Health and Ageing acknowledged:

> The existing inconsistency in privacy regulation makes specific national projects such as Health*Connect* difficult to implement, as there is confusion about which principles apply and under what conditions. As a national network, Health*Connect* needs to have the same privacy rules in force across the private and public health sectors, and across all jurisdictions. This is particularly an issue in the health environment where individuals continually move between the private and public sectors and where providers will routinely deliver health care services in both sectors.[74]

5.53 That is, in contrast to the current privacy regime, a complete set of laws is required that provides uniform levels of protection and procedures nationwide. A readily accessible complaints system is also required to deal with privacy issues on an Australia wide basis.[75]

Development and implementation of a National Health Privacy Code

5.54 To this end, federal, state and territory governments have moved to develop a proposed National Health Privacy Code (the Code) as the national set of rules for the handling of personal health information by all Health*Connect* participants in both sectors throughout Australia. The aim is to provide a set of health-specific privacy principles that can be implemented nationally, harmonising health privacy protection.[76]

---

73 See HealthConnect, *HealthConnect – an overview (updated December 2004),* p. 10. Copy at http://www.healthconnect.gov.au/pdf/overviewDec04.pdf. See also Senator The Hon. Eric Abetz, Special Minister of State, *Privacy Key in E-Government*, media release A0523, 6 June 2005; James Riley, "Abetz calls for privacy review", *The Australian,* 7 June 2005, p. 30.

74 Department of Health and Ageing, *Submission 34,* Attachment, p. 30.

75 Moira Paterson, 'Developing privacy issues in the growing area of health IT', *Australian Health Law Bulletin*, Vol.13, No. 8, May 2005, p. 93.

76 Details are at http://www7.health.gov.au/pubs/nhpcode.htm. The Code establishes a set of National Health Privacy Principles (NHPPs). These govern dealings with 'health information' and are similar to the NPPs established by the Privacy Act. Key differences are NHPP 10, which concerns the transfer or closure of a health service provider's practice, and NHPP11, which set out when health information can be made available to other health service providers. The Code was developed by a National Health Privacy Working Group established by Federal, State and Territory Health Ministers. The Working Group recently concluded public consultations on a draft Code. See HealthConnect, *HealthConnect – an overview (updated December 2004),* p.10. See also Moira Paterson, 'Developing privacy issues in the growing area of health IT', *Australian Health Law Bulletin*, Vol. 13, No. 8, May 2005, p. 93.

5.55 Submissions generally supported the development of the Code.[77] However, this support appeared to be conditional on the Code achieving a higher standard of privacy protection and uniform application and enforcement.[78]

5.56 In this regard, it was argued that the status of the Code, its contents and how and where it would fit into the existing federal, state and territory legal frameworks had to be clarified.[79] The main concern appeared to be that the Code's success was dependent on the agreement of federal, state and territory governments. As the OPC noted:

> The success of a national code will depend critically on how it is implemented. Achieving consistency would involve all jurisdictions implementing the code unamended and in the same manner.[80]

5.57 The APF also advised the committee that:

> this initiative, which already appears to have stalled, will be wasted without a strong commitment by all interested parties to adopt the National Code as the basis for their own laws or rules, without further 'tinkering'.[81]

5.58 The Australian Government can adopt the Code as a schedule to the Privacy Act or by amending the NPPs to incorporate the provisions of the Code.[82] However, the committee understands that either approach will in effect only apply the Code to the agencies subject to that Act – that is, Australian Government agencies and relevant private sector organisations that handle health information. To achieve a consistent national approach across all jurisdictions and all health care sectors, the Australian

77 See, for example, Law Institute of Victoria *Submission 37*; Centre for Law and Genetics, *Submission 6*; Australian Medical Association, *Submission 9*, p, 4; Australian Privacy Foundation, *Submission 32*, pp 8-9.

78 The Australian Medical Association, for example, urged that privacy law be made uniform across the Australian jurisdictions for both the private and public sector and called for a replacement set of nationally coordinated health specific privacy principles, or an overarching national health privacy code. Australian Medical Association*, Submission 9*, p. 4.

79 Australian Medical Association*, Submission 9*, p. 15.

80 OPC review, p. 69.

81 Australian Privacy Foundation**,** *Submission 32,* pp 8-9.

82 The OPC noted the latter option would entail one set of privacy principles to regulate the handling of health information, which address somewhat national consistency issues. However, it would also mean longer and more complex principles and run counter to the aim of providing broad principles of general application. OPC review, pp 69-70.

Government must seek the agreement of all other jurisdictions to adopt the code in the same way.[83]

5.59 In light of the above, the OPC has recommended that:

> The Australian Government should consider adopting the National Health Privacy Code as a schedule to the Privacy Act. This would recognise the Australian Government's part in the consistent enabling of the Code. Should agreement not be reached by all jurisdictions about implementing the Code, the Australian Government should still consider adopting the Code as a schedule to the Act to provide greater consistency of regulation for the handling of health information by Australian Government agencies and the private sector.[84]

5.60 By taking this approach, the OPC considered that the Australian Government could provide national leadership in this complex area and, in the absence of unanimous intergovernmental agreement, set a de-facto national standard for health privacy.[85]

Amendments to the Privacy Act

5.61 Some submissions called for a number of changes to Privacy Act before the National Health Privacy Code is issued. These changes included those outlined below.

Amendment of the primary purpose / consent requirement.

5.62 As explained previously, NPP 2 regulates the use and disclosure of personal information, including health information. It provides that uses or disclosures of personal information are limited to the purpose for which the information was initially collected (the 'primary purpose'), unless a prescribed exception applies.[86] In applying NPP 2, the OPC has interpreted the primary purpose of collecting health information by a health service provider to be the main or dominant reason why the patient is seeking assessment, treatment or care at that time. In doing so, the OPC has stressed that the current arrangements allow health service providers to provide care in the

---

83 OPC review, pp 68-70. No evidence was presented to the committee on the Commonwealth's constitutional powers to enact unilaterally a national health privacy regime binding on state and territory agencies as well as the private sector. State and territory legislation purporting to regulate health records may be inconsistent at least to the extent that it imposes obligations on the same organisations covered by the Privacy Act. See section 3 of that Act. See also OPC review, p. 45. Regulations could be made under the Privacy Act prescribing an instrumentality of a state or territory as 'an organisation' for the purposes of the Act and, by this means, the operation of the Code could be extended to the state and territory public sector health providers. However, this may only occur at the request of the relevant state or territory government. Section 6F(3)(a) of the Privacy Act. See Centre for Law and Genetics, *Submission 24*, p. 6.

84 OPC review, Recommendation 13, p. 9.

85 OPC review, p. 68.

86 There are a range of exceptions to this general rule. The exception at NPP 2.1(a) provides that health information can be used or disclosed for another purpose where this is directly related to the primary purpose and the individual would reasonably expect the use or disclosure. OPC review, p. 263.

manner they consider appropriate for the individual they are treating, having regard to that person's needs and views. Doctors are free to ask - and patients are free to agree either explicitly or implicitly - that patients' health information be used in a more holistic manner.[87]

5.63 Submissions received by the committee argued that limiting the use and disclosure of health information to the collection and use for the single purpose of each episode of care is unworkable and counterproductive. Doing so, it is claimed, interferes with the delivery of holistic health care, obstructs the appropriate management of patients health (for example, by impeding the ability of treating doctors to consult with each other on clinically relevant information) and conflicts with doctors professional and legal obligations towards their patients. For these reasons, it is argued that NPP 2 should be amended to recognise that the 'primary purpose' of collection of health information by doctors is the 'health care and well being' of the patient.'[88]

5.64 The OPC considered these concerns in its review of the private sector provisions of the Privacy Act. It canvassed various options that might address such concerns – such as amending NPP 2 as recommended above or the OPC issuing binding or non-binding guidelines to re-interpret NPP 2 as required. However, the OPC concluded that the current approach was preferable as it provided the necessary flexibility to cover the myriad of relationships between health professionals and their patients. Broad concepts such as 'health care and well being' could also create problems in defining appropriate limits on future disclosure and use. The OPC was concerned that individuals (as patients) may lose the ability to negotiate and enforce alternate health information-handling arrangements.[89]

5.65 The OPC did, however, recognise that it had to provide more effective guidance to assist health services to understand how NPP 2 can operate.[90]

Patient access to medical records

5.66 The AMA expressed concern at the access rights granted to patients by the NPPs, especially when mental health issues are involved.[91] It argued that the NPPs need to take account of the potential for interference with the therapeutic relationship and the patient harm that can arise from patients accessing their medical records. NPP 6 currently allows organisations to withhold access if access would pose 'a serious threat to the life or health of any individual'. The AMA argued that this threshold is

87 See OPC review, pp 263 – 268**.** A holistic approach to healthcare encompasses the idea of taking into account the past experiences and healthcare history of a particular person, and trying to project into the future their likely healthcare needs. See the evidence of the Mental Health Privacy Coalition cited in the OPC review. OPC review, p. 264.

88 Australian Medical Association, *Submission 9*, pp 7-8 and p. 23 of Attachment.

89 OPC review, pp 267-268.

90 OPC review, Recommendations 77 and 78. p. 20.

91 Australian Medical Association, *Submission 9*, p. 7.

too high. That is, it does not protect private or preliminary views recorded in diagnosis and development and formulation of a treatment program. These can be misinterpreted and access can have adverse consequences for patients.[92] The AMA therefore recommended the NPP should be amended to allow patient information to be withheld where access could cause patient harm or interfere with a treatment protocol.

5.67 The OPC has acknowledged that circumstances can exist when access to medical records may cause a breakdown in a therapeutic relationship, which may in turn constitute a serious risk to the patient's health. However, the OPC does not see this as justification to change the law. It noted that the NPPs allow organisations to deny access where it would have an unreasonable impact on the privacy of others. In its view, this extended to the private and preliminary views of therapists and doctors. Nevertheless, in light of the above-mentioned concerns, the OPC undertook to develop further guidance on the operation of NPP 6 to clarify that a serious threat to a therapeutic relationship could constitute 'a serious threat to life or health' for the purposes of that NPP.[93]

Access to health information by care givers

5.68 The AMA also argued the Privacy Act's access provisions, together with restrictions on third party access to health information, fail to account for the needs of care givers to access information about those under their care. Carers, for example, need to know what medication their patient is required to take, the patient's condition on discharge from hospital, what problems they may encounter, and details of follow up appointments. Disclosure of this information to the carer, it is argued, is necessary for the patient's ongoing care, whether or not the patient consents. Access, it is suggested, is especially difficult for informal arrangements where a person with a decision making disability is assisted by a spouse, carer, family members or a friend.[94]

5.69 These concerns were considered by the OPC in its review of the private sector provisions of the Privacy Act. The OPC concluded that the Privacy Act and NPPs made appropriate provision for the disclosure of an individual's health information to carers, family members and other 'responsible' persons. However, the OPC undertook to develop further and more practical guidance on the operation of these provisions.[95]

Parental access to children's medical records

5.70 The AMA also raised its concerns regarding the development of legislation by the Australian Government which would give parents access on request to all information held by Health Insurance Commission concerning their children aged less than 16 years. The committee was advised that this decision is based on the premise

92 Ms Pamela Burton, Australian Medical Association, *Committee Hansard*, 20 May 2005, pp 19-20. See also Australian Medical Association, *Submission 9*, p. 9.

93 OPC review, pp 117 - 118, Recommendation 30.

94 OPC review, p. 213.

95 OPC review, pp 214 - 215.

that, in the ordinary course of events, parents should have a right to access information about their children, especially when it relates to their children's health and welfare.[96] However, the AMA argued that:

> The adverse consequences of this legislative proposal may outweigh the benefits. In circumstances where the parent wishes to access their child's records without the consent of the child, there is a risk that legislating to grant access to such records may adversely affect the relationship between the young patient and his or her doctor. It could discourage some young people in need of help and advice from attending their doctor or being candid in the consultation.[97]

5.71 The OPC was prevented from considering issues concerning the privacy rights of children during its review of the private sector provisions of the Privacy Act, including provisions relating to health. The terms of reference expressly excluded 'children's privacy' from that review. However, the OPC's report of that review stated in its discussion of the access rights of carers, that, in respect of children, the child's parents generally have responsibility for decision-making on their behalf.[98]

Incorporating Public Interest Determinations exemptions into the legislation

5.72 Submissions received by the committee argued that a number of Public Interest Determinations (PIDs) issued by the Privacy Commissioner should be made indefinite by incorporating the exemptions they provide into the legislation.[99] The PIDs concerned exempt health service providers, in certain circumstances, from complying with NPP 10.1, which limits the collection of sensitive information without consent. The concern is that these PIDs operate for only a finite time, but deal with an enduring element of providing quality health care. They relate to the collection of information on family and social histories and from the Health Insurance Commission's Prescription Shopping Information Service.[100]

---

96 Australian Medical Association, *Submission 9*, p. 14. See also Festival of Light, *Submission 30*, p. 6.

97 Australian Medical Association, *Submission 9*, p. 14 and p. 26 of Attachment A.

98 OPC review, p. 213.

99 Australian Medical Association, *Submission 9*, p. 10 See also Department of Health and Ageing, *Submission 34*, p 21. Public Interest Determinations (PIDs) enable the Privacy Commissioner to reduce the privacy protections of one or more of the National Privacy Principles (NPPs) in certain circumstances.

100 The Commissioner issued PIDs to enable doctors in certain prescribed circumstances to collect information necessary to obtain an individual's family, social or medical history during the provision of a health service. A PID was also issued to allow doctors to obtain information from the Health Insurance Commission's Prescription Shopping Information Service. The Service allows doctors who suspect a patient of seeking to obtain medicine in excess of medical need to check records held by the Pharmaceutical Benefits Scheme showing prescriptions issued to the patient. This information was considered a critical part of providing assessment, diagnosis and treatment to the individuals concerned. Obtaining the consent of third parties to collect this information, and notifying those individuals about these collections, was considered impractical, inefficient and detrimental to the provision of quality health outcomes. See OPC review, pp 273 -274.

5.73 The OPC has reported that there is a general consensus that the PIDs concerning the collection of family, social or medical histories are necessary and that they are operating smoothly. It recommended that the Australian Government should consider amending NPP 10 to include an exception that mirrors their operation. Importantly, the OPC also recommended that the government also consider undertaking consultation on limited exceptions or variations to the collection of family, social and medical history information, particularly with regard to genetic information and the collection practices of the insurance industry.[101] The OPC did not appear to consider the PID concerning the Prescription Shopping Information Service.

Penalties for breaches of privacy

5.74 It was also argued that the Privacy Act should be amended to provide penalties for breaches of privacy, especially for unauthorised disclosure of personal health information. The Department of Health and Ageing advised that, 'given the highly sensitive nature of personal health information, and the potential for personal and social harm that can arise from misuse of such information, there is strong support among consumer and provider groups for penalties for breaches of privacy.'[102]

Deceased persons

5.75 It would appear that the Privacy Act effectively only applies to information concerning living persons.[103] The Department of Health and Ageing advised the committee that it supports the inclusion of deceased persons who have been dead for 30 years or less within the scope of the Act, as proposed in the above-mentioned National Health Privacy Code.[104] The Australian Law Reform Commission and the Australian Health Ethics Committee have also recommended that the Privacy Act be amended to cover an individual's genetic information for 30 years after they die. State privacy laws and federal archival and freedom of information laws currently protect an individual's personal information for up to 30 years after death. Extending coverage in the Privacy Act in similar terms would, it is argued, bring that Act into line with this legislation and create greater national consistency.[105]

5.76 The OPC has recommended that the Australian Government consider, as part of a wider review of the Privacy Act, whether the jurisdiction of that Act should be extended to cover the personal information of deceased persons. It did so as, in its view, there may need to be greater consideration of the policy rationale for protecting an individual's personal information for up to 30 years after death.[106]

101 OPC review, Recommendations 81 and 82, p. 20.

102 Department of Health and Ageing, *Submission 34*, p. 21.

103 OPC review, p. 281.

104 Department of Health and Ageing, *Submission 34*, p. 21.

105 OPC review, pp 281-283.

106 OPC review, p. 284.

Contractor provisions

5.77 It was put to the committee that the provisions of the Privacy Act relating to contracted service providers require amendment. Section 95B of the Act generally requires Australian Government agencies to ensure Commonwealth contracts prohibit the contracted service provider from doing an act, or engaging in a practice, that would breach an IPP if done or engaged in by the agency itself. This extends to subcontracts.

5.78 The result is that organisations contracted by the Australian Government (or subcontracted by an Australian Government contractor) can be required to comply with three sets of privacy principles: the NPPs which apply to them in their capacity as private sector organisations; the IPPs which apply to them under contracts granted in accordance with section 95B of the Privacy Act; and any applicable state or territory privacy laws.[107]

5.79 As the Department of Health and Ageing explained, the application of these requirements are complex and confusing. The Department conceded that the NPPs and the IPPs have provisions in common so that compliance with one may ensures compliance with the other. However, it stressed that there are differences and that the above-mentioned combined regime is typically described as a 'minefield'. In the Department's view, it would be much simpler and practicable to require Australian Government contractors to abide by the NPPs.[108]

5.80 Similar concerns were raised with the OPC during its review of the Privacy Act's private sector provisions. The OPC recommended that the Australian Government consider reviewing 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. In its view, this would address the issues surrounding government contractors.[109]

Medical research

5.81 The Privacy Act generally provides health information may be collected, used and disclosed without consent for the purpose of research, provided certain criteria are met. The NPPs generally permit organisations to collect health information without consent in limited circumstances provided the information is required for: research (including compilation or analysis of statistics) relevant to public health or public safety; or the management, funding or monitoring of a health service. Health

107 Department of Health and Ageing, *Submission 34*, p. 13.

108 Department of Health and Ageing, *Submission 34*, pp 13-15. The Department, for example, identified inconsistencies and confusion that have arisen in the context of Australian Government funded Aboriginal health services. It drew attention to circumstances when compliance with the NPPs alone would, in the appropriate circumstances, allow a doctor to discuss the care of a patient with a relative without the patient's consent, but compliance with the IPPs would not. See OPC review, p. 39.

109 OPC review, Recommendation 5, p. 8.

information may only be collected without consent for these purposes if obtaining consent is impracticable, and de-identified information (ie, information which cannot identify the persons it concerns) would not be sufficient. Where these preconditions exist, collection must be carried out either according to guidelines issued under the Privacy Act, or in accordance with binding rules of confidentiality issued by a competent health or medical body, or as required by law.[110]

5.82 The above-mentioned guidelines authorise Human Research Ethics Committees (HRECs) to permit identifiable health information to be used without consent for the purposes of approved research activities if the HREC is satisfied that the activities are substantially in the public interest and outweigh any concerns about privacy protection. Compliance with the guidelines is reported annually to NHMRC. In turn, the NHMRC reports this information to the OPC.

5.83 Submissions received by the committee maintained that the above requirements were unduly restrictive and were hindering important research.[111]As the OPC itself noted:

> There is considerable evidence that key researchers, especially epidemiological researchers, consider that the current balance between privacy and the public benefit of research is too heavily weighted in favour of individual privacy to the detriment of research.[112]

5.84 Concerns raised by researchers include those listed below.

Undue restrictions on secondary use of data

5.85 Some submissions criticised the requirement that personal information only be used or disclosed for research relevant to 'public health or public safety' and only where it was 'impracticable' to seek consent. It was argued that research should be permitted under strict protocols where it is in 'the public interest.' It was also suggested that personal information should be able to be used or disclosed where obtaining consent is not viable, would cause unnecessary anxiety, or where the scientific value of the research would be prejudiced.[113] Submissions also noted that equivalent legislation overseas was less restrictive. The NHMRC explained that:

> Canadian legislation permits agencies to disclose personal information without the individual's consent, for research, if it is satisfied that the research cannot be achieved with non-identifying information and the researcher obtains an undertaking that the information will not be disclosed in an identifying way. The New Zealand Act and Code permit such disclosure if an agency believes on reasonable grounds that it is neither

110 See OPC review, pp 200-201.

111 See, for example, Queensland Institute of Medical Research, *Submission 13*, p. 2; NHMRC *Submission* 20, pp 7-8; Australian Medical Association, *Submission 9*, pp 13-14.

112 OPC review, pp 201-208.

113 OPC review, p. 203. Australian Medical Association, *Submission 9*, pp 13-14.

> desirable nor practicable to seek consent and the information will not be used in an identifying way in research.[114]

Complexity and confusion

5.86 The committee also received evidence that the fragmented approach to privacy regulation in Australia (described elsewhere in this report) is a major impediment to medical research.[115] The Queensland Institute of Medical Research, for example, explained that research teams, especially those conducting multi-centre research, must deal with multiple different pieces of legislation, all with the same intent, but with subtly different wording that can have considerable impact upon the conduct of research.[116]

5.87 Similar concerns were raised with the OPC. It received evidence that the Privacy Act's private sector provisions have made the process of undertaking research more difficult. The provisions, it is argued, slow down approval processes and have an impact on gaining access to, and collecting, data. As the OPC explained:

> Submissions … point to the complexity of the privacy regime in Australia including both within the Privacy Act and between Commonwealth and state legislation and the impact this is having on health and medical research. They say, for example, that the co-existence of the NHMRC's section 95 (public sector) and section 95A (private sector) guidelines and the interaction between the IPPs and the NPPs has created some confusion for researchers and consumers. Also they say that that interpretation and implementation of Commonwealth and state privacy legislation is compromising individually and publicly beneficial research and health care. Problems include that private sector organisations are making incorrect decisions and adopting a highly conservative approach to privacy compliance.[117]

5.88 The committee also received evidence from the NHMRC that the reporting and decision making obligations imposed on HRECs were onerous. The OPC also noted evidence of inconsistencies in the way various HRECS exercised their obligation to weigh up the benefit of a research proposal versus the threat to individual privacy.

5.89 Compounding the above problems are the apparent difficulties researchers experience in determining what data or information is de-identified data and is therefore not subject to the Privacy Act or the NPPs.[118]

5.90 The Queensland Institute of Medical Research suggested that many of the difficulties experienced by medical researchers and members of HRECs in working

---

114 NHMRC, *Submission 20* p. 3.

115 See sources at footnote 111.

116 *Submission 13,* pp 6-7. See also Department of Health and Ageing, *Submission 34*, p. 21.

117 OPC review, p. 201.

118 See this regard pp. 205, 208 of the OPC report.

within privacy provisions stem from inadequate training and a lack of knowledge or awareness. The importance of adequately resourced OPC was again raised as an issue. The Institute argued that 'a national education program and rapid access to advice from a well-resourced Federal Privacy Commissioner would be an extremely valuable service to groups in the health research sector'.[119]

5.91 The OPC report detailed a number of possible options for reform of the privacy provisions affecting medical research. However, noting the complex issues involved, it urged the Australian Government, as part of a wider review of the Privacy Act, to determine, with appropriate consultation and public debate, what is the appropriate balance between facilitating research for public benefit and individual privacy and right of consent.[120]

Responding to overseas emergencies

5.92 Another issue raised during the committee's inquiry related to impediments, under the Privacy Act, to the ability to respond to overseas emergencies. In particular, the committee received evidence from the Australian Red Cross (ARC) and DFAT in relation to the Privacy Act's impact on information-sharing between government and non-government agencies involved in response and recovery in emergency situations overseas.[121]

5.93 DFAT identified privacy-related impediments which had affected its administration of the Australian Government's response to overseas crises (including September 11, the Bali bombings and the recent Boxing Day tsunamis).[122] DFAT submitted that the privacy legislation had impeded DFAT's ability to:

- access personal information held by other government agencies to assist in its location, identification and assistance efforts; and
- provide personal information to other government agencies directly involved in the crisis response.[123]

5.94 For example, DFAT submitted that:

> To meet our consular obligations, it would be useful to be able to access the records of airlines and travel agents regarding the travel plans, hotel reservations, and therefore general whereabouts, of Australians overseas. This information could, for example, confirm which Australians were booked in hotels directly affected by the Boxing Day tsunami. In response to inquiries, DFAT has been advised that airlines and travel agents are unable to disclose personal information because of restrictions in applicable privacy codes or the National Privacy Principles.[124]

119 Queensland Institute of Medical Research *Submission 13*, p. 7.

120 OPC review, Recommendation 60, pp 210-212.

121 See DFAT, *Submission 39*, pp 5-7 and ARC, *Submission 44*.

122 *Submission 39*, p. 5.

123 *Submission 39*, p. 5.

124 *Submission 39*, p. 6.

5.95 DFAT also noted that the Privacy Act had impeded its ability to provide personal information to other government bodies who requested information to ensure inappropriate action is not taken against affected Australians. For example, Centrelink had wanted to avoid taking action to cancel regular social security payments to victims, or pursuing persons affected by the tsunami for overdue payments.[125]

5.96 DFAT concluded that:

> The expectation of the Australian community is that there will be a whole-of-government response to the crisis and that government agencies are working collaboratively to achieve the best outcomes for affected Australians. Constraints under the Privacy Act limited DFAT's ability to provide personal information to some bodies that requested it, particularly those without specific information-gathering powers and State or Territory bodies. Except in a few cases, the Privacy Act does not allow DFAT to automatically share information on those persons affected or unaccounted for in an overseas disaster with other government agencies, which deliver services to these individuals.[126]

5.97 A representative of DFAT expanded on the situation encountered in relation to the Boxing Day tsunamis:

> We had about 87,000 phone calls from members of the Australian public expressing concern about the whereabouts of family members and friends. From that, we developed a list of about 14,000 Australians who we judged may have been in the areas affected by the tsunami. Tracking down 14,000 Australians and confirming their safety is an extremely difficult task. It is one that we could not do on our own. It was very important that we were able to get as much information as we possibly could about where those individuals might have been at the time to help us to get a clearer picture about the risk that they may have been in the immediate vicinity of the tsunami.[127]

5.98 The representative noted that information sharing between government agencies, such as with the Department of Immigration and Indigenous Affairs, was generally good. However, he also observed that there were some limitations, and that the information sharing 'was not always as quick as we would have liked' because they had needed to ensure that they had the appropriate authority under the Privacy Act for the exchange of information between agencies.[128] However, the representative noted that the situation in relation to the private sector was more problematic:

> The real issue…was getting information from private sector organisations, particularly airlines and travel agencies. That is something we are looking into now. There is a working group process, being led by the Attorney-General's Department, looking at the extent to which new flexibility needs to be built into the [A]ct or into the application of the [A]ct

125 *Submission 39*, p. 6.

126 *Submission 39*, p. 7.

127 *Committee Hansard*, 20 May 2005, p. 4.

128 *Committee Hansard*, 20 May 2005, p. 4.

> to help us with the management of information with privacy issues in times of crisis...We do have not a resolution to that yet, but that is something we are following up.[129]

5.99 The ARC argued that in emergency situations, the need for information sharing also extends to non-government organisations engaged in disaster recovery.[130] The ARC submitted that the Privacy Act had imposed significant impediments to its provision of disaster relief. In particular, it cited problems associated with the distribution of assistance by the ARC to Australian victims of the 2002 Bali bombings. In particular, the ARC submitted that some of the issues that it had encountered included:

- the ARC was unable to access lists of deceased, injured and missing which were held by DFAT. While ARC liaised closely with DFAT, privacy legislation prevented sharing of this information;
- the ARC was unable to share its own lists of deceased and injured although requested by some state and territory governments, which did not have comprehensive lists;
- some victims were registered on the National Registration and Inquiry System (a computerised victim registration and inquiry system operated by ARC), but because of the extent of their injuries were unable to give permission to share this information; and
- the ARC needed to seek individual client permission to share even basic information about assistance provided.[131]

5.100 The ARC argued that this inability to share information in such a crisis situation had resulted in an additional barrier to providing assistance to affected persons at a time when that assistance was most needed. The ARC also noted that it had to develop its own list of deceased and injured, compiled through advertisements, media, web searches, word of mouth and referral. Finally, the ARC observed that many affected Australians expressed surprise and concern about having to provide the same information to many different agencies and did not understand why this information could not be provided once and then shared across relevant agencies.[132]

5.101 Secretary General of the ARC, Mr Robert Tickner, put the problem in context:

> …in the aftermath of the disaster that has occurred, someone with horrific injuries who has to tell their story to authorities and to others and who then seeks relief. The person's injuries may range from modest to severe, across a range of possibilities, but, whatever the severity, they have been through a terrible trauma. They have told their story and telling the story just adds to their stress levels. The problem that people found is that they had to tell their story not once, but they had to tell it often to a range of different authorities who might be there to help them for one reason or another. I

129 *Committee Hansard*, 20 May 2005, p. 4.

130 *Submission 44*, pp 2-3.

131 *Submission 44*, p. 2; see also Mr Robert Tickner, *Committee Hansard*, 22 April 2005, pp 30-31.

132 *Submission 44*, p. 2; see also Mr Noel Clement, *Committee Hansard*, 22 April 2005, p. 31.

> guess we are here, motivated by concern for the victims, to look for a simplified procedure that does not result in a sweeping away of people's rights to privacy but, in the very limited circumstances of this kind of emergency, provides some practical pathway forward that assists in making people's lives less stressful than it might otherwise be.[133]

5.102 The ARC argued that there is a need to amend the Privacy Act to enable sharing of information across agencies engaged in emergency response and ongoing disaster recovery functions.[134] Mr Greg Heesom of the ARC suggested that possible solutions could include a PID exemption by the Privacy Commissioner, or an amendment to IPP 11 to provide a specific limited exemption for emergency disaster situations.[135]

5.103 The OPC review also examined the issue of the Privacy Act's impact on responses to large scale emergencies.[136] For example, the OPC review noted the problems encountered during the aftermath of the tsunami disaster in December 2004:

> In an attempt to locate missing family and friends, many Australians contacted airlines to find out whether the missing had continued flying after the tsunami hit. Such information, which is readily available to the airlines, if disclosed would normally appear to be a breach of NPP 2. The aftermath of the tsunami placed organisations in the position of balancing the right of an individual to privacy while also having the capacity to allay the fears of many relatives and friends of those missing. Disclosure of personal information by airlines in situations such as presented by the tsunami could therefore be in breach of NPP 2.[137]

5.104 The OPC review also observed that the Privacy Act received criticism in the media after the tsunami disaster 'for lacking commonsense and for being unable to anticipate and cope with the extent of the tsunami disaster.'[138]

5.105 After considering a number of options,[139] the OPC review concluded that:

> Privacy laws should take a common sense approach. There needs to be an appropriate balance between the desirability of having a flow of information and protecting individual's right to privacy. In developing an exception to disclosure for cases of national emergencies, consideration should be given to the seriousness of the privacy breach versus that of protecting privacy.[140]

---

133 *Committee Hansard*, 22 April 2005, p. 31.

134 *Submission 44*, pp 2-3.

135 *Committee Hansard*, 22 April 2005, p. 32. IPP11 currently provides a narrow exemption allowing for disclosure in limited circumstances to prevent a serious and imminent threat to life or health.

136 OPC review, pp 234-238.

137 OPC review, p. 234.

138 OPC review, p. 235.

139 See further OPC review, pp 235-237.

140 OPC review, Recommendation 68, p. 237.

5.106 The OPC review also observed that:

> In large scale emergencies, the consequences of disclosure should be compared to the consequences of non-disclosure. Consideration also needs to be given to the potential identity fraud that may occur during such a time, especially if disclosure is allowed to the media.[141]

5.107 The OPC recommended that the Australian Government consider:

- amending NPP 2 to enable disclosure of personal information in times of national emergency to a 'person responsible'
- extending the NPP 2.5 definition of 'person responsible' to include a person nominated by the family to act on behalf of the family
- amending the Privacy Act to enable the Privacy Commissioner to make a Temporary Public Interest Determination without requiring an application from an organisation
- defining 'National Emergency' as 'incidents' determined by the Minister under section 23YUF of the Crimes Act 1914.[142]

Use of the Privacy Act as a means to avoid accountability and transparency

5.108 The committee also received evidence about the use of the Privacy Act as a means to avoid accountability and transparency. For example, the Victorian Privacy Commissioner, Mr Paul Chadwick, described this as 'misuse of the Privacy Act', observing that:

> There is a lot of what we call in the trade BOTPA…'Because of the Privacy Act.' You will find many incidents of people saying, "We can't give you that, we can't give you this, Because of the Privacy Act," and it won't be because of the Privacy Act. It will be something else.[143]

5.109 Similarly, Mr Ian Cunliffe believed that government departments and agencies have used the Privacy Act to avoid accountability and transparency. Mr Cunliffe argued that:

> In large matters and small, government bodies routinely deny information to inquirers on the asserted basis that the Privacy Act prevents disclosure.[144]

5.110 Mr Cunliffe suggested that private sector entities can also be 'obstructive' when attempts are made to access to information, when often 'no real privacy issue is involved.'[145]

5.111 In the same vein, the APF was concerned that organisations often cited 'privacy laws' as a reason for not doing something they did not want to do for other reasons, even where there was no factual basis for the claim. The APF suggested there should be a sanction for wilful misrepresentation of the Privacy Act, although it

141 OPC review, Recommendation 68, p. 237.

142 OPC review, Recommendation 68, p. 238.

143 *Committee Hansard*, 22 April 2005, pp 8-9.

144 *Submission 7*, p. [1].

145 *Submission 7*, p. [1].

acknowledged that it may be difficult to legislate against misrepresentation of a law's effect, and that some such claims may be based on genuine misunderstanding. The APF also suggested the Privacy Commissioner be empowered to issue 'corrective statements', to be published at the expense of the organisation concerned.[146]

5.112 Ms Anna Johnston of the APF explained further:

> …the phrase 'because of the Privacy Act' has been used inaccurately by organisations, both government and business, as an excuse, usually for not doing something. That practice is frustrating enough for us as privacy advocates as it brings privacy protection into disrepute; however, an even more disturbing development has been the extent to which privacy-invasive proposals are justified or softened in the public's eye through the mere existence of a Privacy Act. That is, the Privacy Act has been used as a shield behind which all sorts of intrusive practices are conveniently sheltered with a bland reassurance along the lines of: 'You can trust us because we are obligated to comply with the Privacy Act.' In this sense, a Privacy Act which is weak, either in its framework or in its enforcement can actually do harm as its mere existence can be used to shut down or sideline public debate or criticism.[147]

5.113 Ms Johnston put forward a current proposal by the Australian Bureau of Statistics (ABS) in relation to the census as an example of this problem. Ms Johnston believed that the proposal would:

> …radically alter both the nature of the census and the role of the Australian Bureau of Statistics in handling personal data about every Australian. In case you are not aware of that proposal, it is for the ABS to replace the anonymous snapshot of the five-yearly census with instead a permanent movie of every Australian's life. That is the language of the ABS itself—to replace the snapshot with a movie. The result will be a centralised, national population database holding the most extensive collection of data on every person, in an identifiable form. Everything from date of birth, sex, religion and occupation to people's history of disease, their immigration movements and their family relationships will, for the first time, be held in the one place by the Australian government.[148]

5.114 Indeed, Ms Johnston argued that:

> This new census proposal is the closest thing yet that we have seen to the old Australia Card scheme…We know that the Privacy Act alone in its current state can do nothing to prevent that proposal nor can the [A]ct alone stand in the way of the inevitable bears being attracted to the honey pot that a national population database presents. Legislation alone cannot protect Australians' privacy. We need informed public debate and absolute political commitment if we are to avoid becoming a surveillance society.[149]

---

146 *Submission 32*, p. 26.

147 *Committee Hansard*, 19 May 2005, p. 13.

148 *Committee Hansard*, 19 May 2005, p. 13. See further ABS, *Discussion Paper: Enhancing the Population Census: Developing a Longitudinal View,* ABS 2060.0, April 2005.

149 *Committee Hansard*, 19 May 2005, p. 13.

5.115 Ms Johnston believed that 'the ABS in its discussion paper on this proposal has sought to reassure the public by sheltering behind the mere existence of a Privacy Act.'[150]

5.116 However, the committee notes that the ABS census proposal has been released for public consultation and will also be subject to a privacy impact assessment, which will also be published.[151]

Law enforcement issues

5.117 The AFP submitted that it had encountered some practical law enforcement issues with regard to the AFP accessing information from organisations subject to the NPPs.[152] In particular, the AFP noted that some organisations, such as utility and service providers, have been reluctant, or have refused, to provide information requested by the AFP for law enforcement purposes.[153] The AFP suggested that this may have a number of causes:

- organisations that are less familiar with the operation of NPPs can be reluctant to assist law enforcement as they are not aware the disclosure 'reasonably necessary for the enforcement of criminal law or a law imposing a pecuniary penalty' is a lawful disclosure;
- provision of such information can be in conflict with business outcomes as it requires organisations to provide information that can be detrimental to commercial interests;
- there are costs associated with complying with a request for information that organisations are reluctant to bear; and
- some organisations are concerned about litigation being commenced by clients whose information has been disclosed to police.[154]

5.118 For example, Mr Trevor Van Dam of the AFP observed that:

> …we do see cases where either organisations are concerned about a future commercial liability, for having passed information on, or they have been concerned about the impact on their commercial activities.[155]

5.119 The AFP noted that while education may have a role to play in raising awareness, this is unlikely to offer a complete solution. The AFP suggested that 'a legislative approach such as a "notice to produce", as is currently available to a

150 *Committee Hansard*, 19 May 2005, p. 13.

151 ABS, *Discussion Paper: Enhancing the Population Census: Developing a Longitudinal View,* ABS 2060.0, April 2005, p. 18.

152 *Submission 42*, p. 3.

153 *Submission 42*, p. 3; see also Mr Trevor Van Dam, AFP, *Committee Hansard*, 20 May 2005, pp 39-40.

154 *Submission 42*, p. 3; see also OPC review, p. 222.

155 *Committee Hansard*, 20 May 2005, p. 43.

number of other government entities, may be a potential solution to these difficulties.'[156]

5.120 Law enforcement issues were also considered by the OPC in its review of the private sector provisions of the Privacy Act.[157] The OPC review recommended that:

> The Office will work with the law enforcement community, private sector bodies and community representatives to develop more practical guidance to assist private sector organisations to better understand their obligations under the Privacy Act in the context of law enforcement activities.[158]

5.121 The AFP supported this recommendation, but observed that 'notices to produce' may also be useful:

> In the context of examining the possibility of notice[s] to produce, we are aware of the fact that such a facility already exists within other legislation and that operates quite comfortably beside the privacy legislation. In some respects, it helps to clarify for a provider of the information that they have a cover in the context of a formal notice that gives them some comfort against future claim.[159]

5.122 Mr Trevor Van Dam continued:

> …we think it is appropriate to have a look at the application of that within some other legislative arrangements. Over the next period our view is that we would examine that and have a look at whether or not, for argument's sake, changes to the [Australian Federal Police Act 1979] or Crimes Act might be required.[160]

Privacy issues for care leavers

5.123 Care Leavers of Australia Network (CLAN) raised concerns that the Privacy Act unduly restricts access to third-party (family) information which may assist care leavers (for example, people who grew up in orphanages and similar institutions) to identify their family and background. CLAN's submission highlighted for the committee the profound impact that the loss of contact with family, siblings and place of origin and the ensuing loss of identity can for those raised in care. Yet, as CLAN noted, the Privacy Act's 'provisions can be used to hinder those wishing to access information relating to their time spent in institutional and other forms of out-of-home care, especially that concerning their biological identities'.[161] As explained elsewhere in this report, privacy laws generally restrict third party access to personal information without consent. CLAN urged the committee to give consideration to

156 *Submission 42*, p. 3.

157 OPC review, pp 219-223.

158 OPC review, Recommendation 65, p. 223.

159 Mr Trevor Van Dam, AFP, *Committee Hansard*, 20 May 2005, p. 43.

160 *Committee Hansard*, 20 May 2005, pp 43-44.

161 Submission *29*, p. 1.

Recommendation 16 of the *Forgotten Australians* report of the Senate Community Affairs Committee.[162] That Committee recommended, among other things, that:

> That all government and non-government agencies agree on access guidelines for the records of all care leavers and that the guidelines incorporate … the commitment to the flexible and compassionate interpretation of privacy legislation to allow a care leaver to identify their family and background.[163]

5.124 The committee notes that the Australian Government has yet to respond to that recommendation.[164]

162 *Submission 29*, p. 6.

163 Senate Community Affairs References Committee, *Forgotten Australians: A report on Australians who experienced institutional or out-of-home care as children*, August 2004, p. 286.

164 It is understood that the Government's response was delayed by the need to await the second report of the 'Forgotten Australians' inquiry. The second report was tabled in March 2005 and covered remaining matters including foster care, children with physical and mental disabilities in care, and other contemporary issues of child welfare and child protection.

CHAPTER 6

RESOURCING AND POWERS OF THE OFFICE OF THE PRIVACY COMMISSIONER

6.1 This chapter will consider issues raised in the course of the committee's inquiry in relation to the resourcing of the OPC, and whether current levels of funding and the powers available to the OPC enable it to properly fulfil its mandate.

Resourcing of the Office of the Privacy Commissioner

6.2 The resourcing challenges faced by the OPC are illustrated starkly by the evidence presented to the committee during the course of its inquiry. On the one hand, there has been a steady increase in the number of privacy-related issues which come within the functions of the OPC; indeed, as the OPC has indicated: 'the introduction of new technologies has increased the range of potential privacy issues within the community'.[1] Yet, on the other hand, there has been no corresponding increase of staff for the OPC.

6.3 In response to a request by the committee to provide staffing numbers for each financial year since 1994-1995, the OPC indicated that it had the same number of staff during the most recent reporting year[2] as it did at the beginning of that decade.[3] A temporary increase in staff numbers during the years 2001-2003 was 'for the purpose of developing and writing guidelines and other information for the commencement of the private sector provisions of the Privacy Act.'[4]

6.4 Given the arguably exponential increase in matters relevant to the functions of the OPC, it seems extraordinary that there has been no corresponding increase in staff over the last decade.

6.5 Many submissions expressed concern that the OPC is inadequately funded or resourced, and gave their support to increased funding for the OPC.[5] For example, the AMA believed that 'the OFPC has insufficient resources to investigate and take action in respect of privacy breaches in a timely manner'.[6] The AMA submitted that:

---

1 *Submission 43*, p. 13.

2 That is, 2003-2004.

3 *Submission 43*, p. 3.

4 *Submission 43*, p. 3.

5 See, for example, AEIA, *Submission 16*, pp 2-3; AEEMA, *Submission 26*, p. 3; Mr Roger Clarke, *Submission 28,* p.3 and Attachment p. 9; FIA, *Submission 3*, p. 10; AMA, *Submission 9*, p. 16; APF, *Submission 32*, pp 22-23; ACA, *Submission 15*, pp 15-16; Victorian Privacy Commissioner, *Submission 33*, pp 5-6; Baycorp Advantage, *Submission 43*, p. 16.

6 *Submission 9*, p. 16.

> The work of the OFPC has occurred despite the severe lack of resources provided to it to investigate and rectify privacy complaints, carry out educative campaigns, take action on its own initiative, and be proactive in the administration of the Act.[7]

6.6 Mr Roger Clarke argued that the OPC has had its responsibilities increased in recent years, without a corresponding increase in resources:

> The OFPC has had its responsibilities greatly increased, and has no more resources, and possibly fewer resources, than prior to the addition of the private sector to its purview.
>
> …
>
> The impact of this has been that the OFPC is prevented from fulfilling its responsibilities. It conducts few audits, its replies to complaints and submissions are very slow, it is unable to respond quickly to sudden demands, and it is able to conduct very little own-volition research and investigation.[8]

6.7 Some submissions suggested that technological advancement would only exacerbate this situation.[9] For example, the AEEMA suggested that the OPC itself needed a 'better understanding…of the rapid advancements in technology and their obvious benefits to business efficiency and community convenience'.[10]

Failure to address systemic issues

6.8 Several submitters noted that, due to resource constraints, the OPC has been forced to concentrate on dealing with individual consumer complaints, at the expense of other strategic functions, such as audits, policy making, enforcement and education.[11] For example, the ACA suggested that the OPC should be doing more in terms of enforcement action. However, it noted that this would require greater resources to allow the OPC to meet its complaints load and to discharge other duties.[12] Indeed, the OPC itself has reported that resources have been reallocated from audit activities to other 'priority areas'.[13]

6.9 The ACA's observation in relation to strategic direction issues regarding the OPC was as follows:

---

7 *Submission 9*, p. 16.

8 *Submission 28*, p. 3.

9 See, for example, AMA, *Submission 9*, p. 16.

10 *Submission 26*, p. 3.

11 See, for example, ACA, *Submission 15*, pp 15-16; APF, *Submission 32*, p. 22.

12 *Submission 15*, p. 16.

13 Office of the Privacy Commissioner, *The Operation of the Privacy Act Annual Report: 1 July 2003 – 30 June* 2004, p. 65; see also Issues Paper, pp 45-46.

> …resource constraints…have bound the Office tightly to one aspect of its compliance role, dealing with complaints from individuals. Public sector audits, inputs to policymaking and effective engagement of public education have all suffered, while at the same time, speedy complaint resolution has proven difficult to deliver. This is acknowledged in the Issues Paper by the OFPC into its review of its own operations, which indicates that having identified complaint handling as a priority the Office diverted resources from other areas of responsibility. This clearly indicates that the strategic direction of the Office has been subverted by short-term contingencies.[14]

6.10 The APF made a similar argument:

> Both by design and by failure to provide the Privacy Commissioner with adequate resources, the regime relies largely on complaints. This is a completely inadequate way of seeking to promote privacy compliance. Many interferences with privacy go unnoticed by the particular individuals involved, and even where they are noticed, they rarely cause such significant harm as to warrant the time and effort of complaining. This does not mean that they are unimportant – the cumulative effect of repeated small scale intrusions is just as corrosive of trust in organisations as a few major privacy breaches.[15]

6.11 The APF contended further:

> Problems that we see constantly repeated over many years are not being adequately addressed. It should not be necessary to keep bringing individual or even representative complaints, which are a very inefficient way of addressing systemic problems.
>
> …
>
> Slavishly giving priority to individual complaints helps fewer people in the long term than using enquiries, complaints and third party referral of issues to identify systemic issues which can then be addressed with own-motion investigation powers (and audit powers in those jurisdictions where they are available).[16]

6.12 The APF also made the point that there is currently no incentive for respondents to make complaints to correct systemic flaws in the privacy regime since '(i)n most cases, the worst outcome for a respondent, regardless of how bad the conduct, is that they must amend the records'.[17] Further:

> There is a lack of information provided to complainants (or their advisers) when raising repeated (or systemic) problems. While the specific

14 *Submission 15*, pp 15-16.

15 *Submission 32*, p. 22.

16 *Submission 32*, pp 22-23.

17 *Submission 32*, p. 23.

> complainant's problem may be resolved, the adviser is rarely informed whether there has been any response to what might be a broader problem with a particular respondent. We understand that the OFPC sometimes provides advice to major respondents that goes beyond anything made public. Consumer advisers should be aware of what that advice is.[18]

6.13 At the public hearing in Melbourne, Ms Loretta Kreet from Legal Aid Queensland also submitted that, in her view, limited resources have resulted in the OPC being overwhelmed by individual complaints, at the expense of addressing more strategic compliance issues:

> I understand that, in a climate where resources are limited, enforcement should be strategic so that the successful enforcement action changes industry practice. If all the office is capable of doing is handling individual complaints then industry practice will not change, because there does not seem to be effective enforcement across the industry.[19]

6.14 The Privacy Commissioner's recent review of the private sector provisions of the Privacy Act considered the OPC's capacity to respond to systemic issues raised in complaints or identified by other means. The review noted evidence suggesting that the OPC's limited focus on systemic issues and its lack of power to deal with these issues 'is out of step with best practice for complaint handlers'.[20] The review also noted that '(a) greater focus on analysing complaints, following up leads, conducting more own motion investigations to identify systemic issues and so on could also feed into education and guidance activities'.[21]

6.15 The review recommended that the OPC 'will consider options for providing more feedback on systemic issues either in advice or guidance or in some form of regular update to stakeholders.'[22]

Flaws in complaints handling process

6.16 Several submissions noted that, despite the OPC's emphasis on the complaints handling process, even that process appears to be under-resourced.[23] In particular, several submissions expressed concern about certain aspects of complaints handling

---

18 *Submission 32*, p. 23.

19 *Committee Hansard*, 22 April 2005, p. 27.

20 OPC review, p. 150.

21 OPC review, p. 150.

22 OPC review, Recommendation 38, p. 162.

23 ACA, *Submission 15*, p. 15; APF, *Submission 32*, p. 22.

by the OPC, particularly the delays in complaints handling.[24] The ACA suggested that the OPC's funding needed to be commensurate with the volume of complaints coming to the OPC.[25] Further, the ACA submitted that:

> …the OFPC has a high rate of discouraged complainants, abandoned complaints and unhappy consumers. Consumers must have confidence that if their rights are flouted, they can easily seek speedy and effective redress. This is not the case for privacy rights in Australia following the passage of the Act.[26]

6.17 EFA made some strong criticisms of the complaint-handling process, arguing that it requires 'greater transparency and considerably more information about the OFPC's views about application of the NPPs needs to be made publicly available'. EFA also expressed concerns in relation to the delays in dealing with complaints:

> We consider the OFPC should be sufficiently well-funded to deal with complaints promptly, and without need to remove staff from other important areas such as policy and auditing of government agencies as has reportedly occurred.
>
> Without adequate complaints handling procedures, backed up ultimately by strong legal sanctions, the P[rivacy] A[ct] will continue to be a generally ineffective and token piece of legislation.[27]

6.18 In response to the committee's questions on notice in relation to private sector provisions complaints, the OPC stated that in the financial year to date, 'the average time it has taken for complaints…to be resolved or closed is 88 working days or 4.5 months'.[28] Further, the OPC stated that in the financial year to date, '99 complaints…have taken more than 12 months to resolve; this represents 12% of all private sector complaints closed in this period'.[29] However, the committee notes that, since these figures only relate to private sector complaints, they may not be an accurate representation of the total number of complaints subject to delayed resolution.

6.19 At the Sydney hearing, Mr Andrew Want, Chief Executive Officer of Baycorp Advantage, told the committee that his organisation is a strong supporter 'of a

---

24 For example, ACA, *Submission 15*, p. 15; ANZ, *Submission 6*, p. 6; FIA, *Submission 3*, p. 9; Legal Aid Queensland, *Submission 31*, p. 5. For example, Legal Aid Queensland reported that '(i)n September 2004 one of our officers was informed by the Privacy Commissioner's Office that they had just started opening files for complaints received in September 2003. A delay of one year or more between the making of a substantive complaint and investigation of the complaint is arguably not acceptable': *Submission 31*, p. 5.

25 ACA, *Submission 15*, p. 16.

26 *Submission 15*, p. 15.

27 *Submission 17*, p. 46.

28 *Submission 48*, p. 11.

29 *Submission 48*, p. 11.

significant investment in the capabilities…and in the resources of the [OPC]'.[30] In particular, Mr Want spoke about the need for increased resources in the area of complaints resolution:

> Certainly in the area of complaints resolution there need to be some additional resources. We feel the commissioner's office and the community would benefit from having additional resources to aid in the policy debate—to help explore the areas that we have been discussing about this very sensitive balance that needs to emerge over the next couple of years between freedom of information and freedom of anonymity, if you like.[31]

6.20 At the Sydney hearing, Mr Timothy Pilgrim from the OPC expanded on this point. He noted the constraints placed on the OPC:

> Under the Act currently it states that, on receiving a complaint such as that, the Privacy Commissioner shall investigate. As you can imagine, that has resource implications if we are looking at that sort of issue. One of the things we would prefer to do is to be able to advise the person that we have received that sort of complaint and will monitor it to see if that is a particular systemic issue and look to see if there is a broader systemic issue over time that we need to resolve rather than having to devote immediate resources to that one particular issue. I am not trying in any way to belittle an individual's complaint—please understand that—but that is just an example of an instance where there is something that you probably would not want to devote an entire person to trying to resolve that at that point.[32]

6.21 The FIA suggested an alternative – and, in its view, preferable – way of dealing with complaints:

> OFPC has acknowledged that it does not have the capacity to deal with complaints within a reasonable time and that the process may lack transparency (including the lack of right of review).
>
> ...
>
> Complaints are most likely to be made to the offending organisation in the first instance. Requiring their examination by the organisation, through a self-audit-self-regulatory process sanctioned through standards of practice that underlie the legislation would ensure appropriate consideration of the complaint and enhancement of community awareness of their rights and methods by which they can exercise them. These methods would be easier, cheaper and more efficient than the current complaint handling by the OFPC.[33]

---

30 *Committee Hansard*, 19 May 2005, p. 3.

31 *Committee Hansard*, 19 May 2005, p. 5.

32 *Committee Hansard*, 19 May 2005, p. 54.

33 *Submission 3*, p. 9.

6.22 The ACA argued that one of the ways in which greater community confidence in protection of privacy rights could be encouraged is by 'more vigorous and apparent enforcement action'.[34] This would encompass further action than 'simple awareness-raising' in order to 'convince consumers that there really is a viable avenue for privacy complaints at the OFPC'.[35] The ACA submitted that:

> This would involve establishment of a resource stream to the Office sufficient to meet the complaints load and to discharge the other duties of the Office in providing policy advice, researching and anticipating innovation, and conducting audits and other active information seeking programs, such as shadow shopping perhaps.[36]

6.23 Further, the ACA argued that:

> …a mechanism should be established that provides a funding stream to the dispute resolution activities of the Office that is commensurate with and scales to meet the volume of complaints coming to the OFPC. Preferably this funding would be provided by a scheme whereby organisations complained against bear the cost. Indeed our preference would be for a separation of the dispute resolution aspects of the Office from its regulatory functions – the two do not always sit comfortably in the same structure. As a regulator the OFPC should have a role in defining and monitoring the effectiveness of A[lterative] D[ispute] R[esolution] functions as well as being required to respond to systemic problems revealed by the individual complaints data.[37]

6.24 The increased availability of dispute resolution processes was a measure supported by others. For example, Legal Aid Queensland submitted that:

> …it would also assist in easing the load on the Commissioner's Office if entities, particularly in the credit reporting area were required to make available an approved internal dispute resolution process. Aggrieved consumers should also have access to efficient no cost external dispute resolution processes either via the Privacy Commissioner or an industry scheme meeting the requirements for external dispute resolution schemes contained in the Australia Securities and Investment Commission Policy Statement 139.[38]

6.25 The ACA stressed that, in its view, the Privacy Act imposes merely a 'bare bones' privacy framework with, for example, no required reporting and no real capacity for the OPC to impose direct cost on industry. However, the ACA raised an

---

34 *Submission 15*, p. 16.

35 *Submission 15*, p. 16.

36 *Submission 15*, p. 16.

37 *Submission 15*, p. 16.

38 *Submission 31*, p. 5.

interesting point in relation to the resourcing issues faced by the OPC and the efforts made by industry to comply with privacy obligations:

> Where we have sympathy with industry is in the point that companies have in many sectors devoted some not-inconsiderable effort to ensuring they meet the prescriptions of the Act in a consistent and reliable way, while the resources assigned to the OFPC to achieve its mission in the private sector are derisory. In our view, while the OFPC has laboured mightily with the scant resources it has been given, the overall impression is that the Government has actually taken its own legislation a lot less seriously than the organisations to which it applies. If this persists, it inspires an atmosphere of demolition by neglect, scarcely a credible position for any organisation, let alone a regulator with an enforcement role, albeit a restricted one.[39]

6.26 The committee notes that the Privacy Commissioner's recent review of the private sector provisions recommended that:

> The Australian Government should consider the strong calls by a wide range of stakeholders for the Office to be adequately resourced to meet its complaint handling functions.[40]

6.27 The Privacy Commissioner's review also recommended that the Australian Government consider amending the Privacy Act to give the Privacy Commissioner a further discretion not to investigate complaints where the harm to individuals is minimal and there is no public interest in pursuing the matter.[41]

6.28 The APF was particularly critical of this recommendation:

> Although at first glance this appears to be a reasonable position, possibly due to limited resources, we do not agree that the Privacy Commissioner should be able to pick and choose which complaints to investigate.[42]

6.29 Amongst other things, the APF pointed out a practical issue that may arise if such an approach were to be adopted:

> …how would the Office determine what 'harm' the person has suffered, or where the 'public interest' lies, without conducting at least a preliminary investigation? The Office's resources may well be taken up debating the relative 'harm' and the 'public interest' between the two parties, instead of just getting on with resolving the matter.[43]

---

39 *Submission 15*, p. 17.

40 OPC review, Recommendation 45, p. 163.

41 OPC review, Recommendation 46, p. 163.

42 *Submission 32B*, p. 5.

43 *Submission 32B*, p. 5.

6.30 The APF submitted that it did not support this recommendation. However, it made the following concession:

> …if recommendation 46 is to be followed, purely on the basis of a measure to allow the Office to focus its resources on complaints that suggest systemic problems, we argue that there must be a corresponding allowance for direct civil action by individuals against organisations that breach the Act.[44]

Awareness and education

6.31 Several submissions noted that there appears to be a low level of awareness among consumers about the privacy legislation and the OPC.[45] These submissions argued that the OPC needs increased resources in order to play a greater role in promoting education and awareness of the Privacy Act.[46]

6.32 For example, the NHMRC noted that the Australian Health Ethics Committee had worked in collaboration with the OPC to develop and conduct a series of training workshops in every capital city to assist ethics committees and researchers to understand relevant guidelines under the Privacy Act.[47] The NHMRC noted that it alone had provided funding for these workshops. It argued that such privacy training should be funded 'largely if not exclusively' by the Privacy Commissioner, as the responsible agency.[48] The NHMRC concluded by recommending that Privacy Commissioner be given sufficient resources to ensure that education and awareness programs can be funded and implemented.[49]

6.33 At the Sydney hearing, the Privacy Commissioner, Ms Karen Curtis, told the committee that her recent review of the private sector provisions of the Privacy Act revealed a general call by all sectors for increased resourcing for the OPC in a variety of areas:

> It is clear throughout the report that there has been a call by all sectors—business large and small, individuals, consumer representatives—for increased resourcing for the office in terms of our complaints handling and also for an education and awareness program. I have made recommendations to the Attorney that he should take into account those strong calls for increased funding for those areas in particular. We have not

---

44 *Submission 32B*, p. 5.

45 See, for example, APF, *Submission 32*, p. 22; ADMA, *Submission 38*, p. 8; Ms Jodie Sangster, ADMA, *Committee Hansard*, 19 May 2005, p. 30. Note also the OPC and ADMA research in relation to this, as discussed in chapter 2.

46 See, for example, AEEMA, *Submission 26*, p. 3; NHMRC, *Submission 20*, p. 9; FIA, *Submission 3*, p. 5; QIMR, *Submission 13*, p. 7; ADMA, *Submission 38*, p. 8.

47 *Submission 20*, p. 9.

48 *Submission 20*, p. 9.

49 *Submission 20*, p. 10.

> developed an education and awareness program, so we have not costed what that might be, so I cannot give you a specific figure.[50]

6.34 Ms Curtis reiterated the importance of promoting awareness and education at the committee's May 2005 Budget Estimates hearing, in response to questioning by the committee in relation to priority funding areas:

> In the review that I recently completed about the private sector provisions it was clear that there was a general call by industry, as well as by the consumers and the government departments and agencies, for increased awareness and education about both the right of individuals and the responsibilities and obligations of business. So I think an education and awareness program would be a priority.
>
> …
>
> Within our current funding we do provide advice and we do have education and awareness. We maintain a web site. We have lists of people that we send information to. We try to communicate as effectively as possible with the wider community, but an integrated education awareness program would be of use.[51]

Powers of the Office of the Privacy Commissioner

6.35 Some submissions and witnesses argued that the powers of the Privacy Commissioner are inadequate. For example, the ACA was of the view that the powers of the OPC are 'too restricted', and argued that the Privacy Commissioner should have greater powers including:

- an audit power in relation to the private sector;
- the capacity to address systemic privacy problems outside the context of resolving an individual complaint;
- the power to fine an organisation that breaches privacy provisions;
- ability to enforce any directions given in relation to findings after an own motion investigation;
- ability to seek court enforceable undertakings; and
- power to issue a standard or binding code to address systemic failings.[52]

6.36 The ACA stated that, while not advocating 'a draconian or a legalistic "black letter" approach', it was of the opinion that 'a credible set of powers and penalties connects the regulator with the legal framework of enforcement, and ensures that

50 *Committee Hansard*, 19 May 2005, p. 54.

51 *Estimates Hansard*, 24 May 2005, p. 60.

52 *Submission 15*, p. 17.

more "light handed" interventions have the weight of possible further action attached to them'.[53]

6.37 Moreover, while acknowledging that its suggested changes may have considerable resource implications, the ACA noted that if changes were implemented, this may result in long-term cost saving measures:

> The prospect of more vigorous regulatory action may well lower the number of complaints over time, while enforceable fines would in fact yield revenue, albeit to consolidated government funds. Coupled with a more industry funded A[lternative] D[ispute] R[esolution] scheme as outlined above, these changes could well mean the OFPC becoming a far more cost-effective instrument.[54]

6.38 The Victorian Privacy Commissioner submitted that the powers, independence, resources and accountability for the OPC should be commensurate with the significance of the right to privacy as a basic human right; and the complexity of OPC's tasks in the contemporary and foreseeable governmental, commercial, social and technological context. The Victorian Privacy Commissioner also suggested that Privacy Commissioner should be able to table reports directly in Parliament.[55]

6.39 The APF submitted that the functions and powers of the Privacy Commissioner are generally adequate, but ineffective due to lack of resources. Nevertheless, the APF recommended a number of extended or additional powers for the Privacy Commissioner, including:

- extending the audit function to compliance by private sector organisations with the NPPs;
- the power to initiate a code of practice to deal with particular issues affecting the private sector;
- the power to selectively require agencies and organisations to publish details of major projects or proposals with significant privacy implications;
- an express role in relation to privacy impact assessments;
- the power to issue or require corrective statements; and
- a more systematic and streamlined complaints process.[56]

6.40 The Centre for Law and Genetics submitted similarly that current enforcement powers in the Privacy Act are 'relatively weak'.[57] At the Canberra hearing, Dr Dianne

---

53 *Submission 15*, p. 17.

54 *Submission 15*, p. 17.

55 *Submission 33*, pp 5-6; *Committee Hansard*, 22 April 2005, p. 5.

56 *Submission 32*, pp 23-24; pp 26-27.

57 *Submission 24*, p. 5.

Nicol from the Centre for Law and Genetics provided the committee with more information on this point and suggested how this might be changed:

> Certainly, at the moment, determinations of the commissioner are not binding on either of the parties. So it is then up to the commissioner or the complainant to bring a further action to the Federal Court and there is another hearing de novo, so it is a fairly lengthy process to get anything in the form of enforceable requirements. One area that might be instructive is schedule 5 of the Broadcasting Services Act relating to censorship of the internet. The provisions in schedule 5 relate to determinations of the Australian Broadcasting Authority. They define them as online provider rules, and those rules are binding such that, if the rules are not followed, it becomes an offence, so it is an offence not to follow the determinations of the Australian Broadcasting Authority. Perhaps a similar procedure could be put in place for the Privacy Commissioner so as to give the determinations of the Privacy Commissioner some binding force.[58]

6.41 The AEEMA also observed that, compared to European Union jurisdictions, the enforcement powers and procedures under the Australian regime 'engender a more subtle approach to breaches.'[59]

6.42 At the Melbourne hearing, Ms Irene Graham from EFA argued that a more prescriptive approach than is currently set out in the Privacy Act would be a preferable approach to enforcing privacy rights:

> …it is [currently] almost impossible for an individual to enforce their supposed privacy rights…So at the moment for an individual to enforce their alleged rights, it is a very complex and expensive exercise. You may be lucky and have the commissioner make a decision quickly and the business just agree to do that—and that certainly does happen with some smaller aspects. But if you have a serious breach of privacy, it is more likely that you will end up having to go to the Federal Court to get the decision heard again. We think that is too hard for most people—too hard and too expensive.[60]

6.43 The Privacy Commissioner's recent review of the private sector provisions also considered many of these issues.[61] The review recommended, amongst other things, that:

- the OPC will consider promoting privacy audits by private sector organisations;[62]
- the OPC will review its complaints handling processes;[63]

---

58 *Committee Hansard*, 20 May 2005, p. 12.

59 *Submission 26*, p. 3.

60 *Committee Hansard*, 22 April 2005, p. 48.

61 See OPC review, pp 125-163.

62 OPC review, Recommendation 39, p. 162.

- the OPC will consider measures to increase the transparency of its complaints processes and complaint outcomes;[64]
- the Australian Government should consider amending the Privacy Act to provide for enforceable remedies following own motion investigations where the Privacy Commissioner finds a breach of the NPPs;[65] and
- the Australian Government should consider amending the Privacy Act to provide a power for the development of binding codes and/or binding guidelines in certain circumstances.[66]

6.44 The APF's response to the Privacy Commissioner's review noted that:

> …less timidity in the presentation of many of the recommendations could have spurred more action by the Government, such that instead of being encouraged to just "consider" doing something…it could have been given the permission as a result of this review to just "do it".[67]

6.45 This is particularly pertinent to many of the recommendations set out above in paragraph 6.43.

6.46 The APF also argued that 'there are few recommendations that could bring about genuine and systemic improvements, such as private sector auditing powers for the [OPC]'.[68]

---

63 OPC review, Recommendation 42, p. 163.

64 OPC review, Recommendation 43, p. 163.

65 OPC review, Recommendation 44, p. 163.

66 OPC review, Recommendation 44, p. 163.

67 *Submission 32B*, p. 3.

68 *Submission 32B*, p. 7.

CHAPTER 7

THE COMMITTEE'S CONCLUSIONS

7.1 The committee is concerned that the Privacy Act is not proving to be an effective or appropriate mechanism to protect the privacy of Australians. The committee considers that a combination of factors are undermining the Privacy Act, including lack of consistency with other legislation; the challenges of emerging technologies; the numerous exemptions under the Privacy Act; lack of resourcing of the OPC; and lack of effective complaints handling and enforcement mechanisms.

A comprehensive review

7.2 The committee therefore considers that there is considerable merit in the recommendation by the OPC that the Australian Government undertake a wider review of privacy for Australians in the 21st century. Some of the matters that should be considered by this review will be discussed further in this chapter. For example, the committee believes that the review should include a 'stock take' of emerging technologies and their privacy implications, and ways in which privacy regulation could be improved to deal with these technologies.

7.3 The committee believes that the most appropriate body to conduct this review is the Australian Law Reform Commission (ALRC), as independent statutory corporation with responsibility for, and a proven track record in, reviewing areas of Commonwealth law reform as referred by the Attorney-General. In particular, the committee notes that, under the *Australian Law Reform Commission Act 1996,* the functions of the ALRC in reviewing Commonwealth law include to simplify the law; remove obsolete or unnecessary laws; eliminate defects in the law; and to ensure harmonisation of Commonwealth, state and territory laws where possible.[1] The committee notes that the ALRC also has extensive experience in undertaking thorough public consultation with key stakeholders. The committee also recognises that the ALRC has relevant technical expertise, having conducted previous inquiries relevant to privacy legislation, including the recent inquiry into the protection of genetic information, and also the 1983 privacy inquiry which became the foundation for the *Privacy Act 1988*.[2]

Recommendation 1

7.4 The committee recommends that the Australian Government undertake a comprehensive review of privacy regulation, including a review of the *Privacy Act 1988* in its entirety, with the object of establishing a nationally

---

1 *Australian Law Reform Commission Act 1996,* s. 21.

2 The Law Reform Commission, *Privacy*, ALRC Report No. 22, 1983; and see also *Privacy and the Census,* ALRC Report No. 12, 1979.

consistent privacy protection regime which effectively protects the privacy of Australians.

Recommendation 2

7.5 The committee recommends that the Australian Law Reform Commission undertake the review proposed in recommendation 1 and present a report to Government and to Parliament.

Consistency

7.6 The committee is greatly concerned at the significant level of fragmentation and inconsistency in privacy regulation. This inconsistency occurs across Commonwealth legislation, between Commonwealth and state and territory legislation, and between the public and private sectors. As mentioned above, the committee believes that this inconsistency is one of a number of factors undermining the objectives of the Privacy Act and adversely impacting on government, business, and mostly importantly, the protection of Australians' privacy. The ALRC review proposed above should consider this issue.

Recommendation 3

7.7 The committee recommends that the review by the Australian Law Reform Commission, as proposed in recommendations 1 and 2, examine measures to reduce inconsistency across Commonwealth, state and territory laws relating to, or impacting upon, privacy.

7.8 Another key area of inconsistency is within the Privacy Act itself – in the two different sets of privacy principles, the IPPs and NPPs, applying to the public and private sectors respectively. The committee agrees that there is no clear policy reason for having two separate sets of principles applying to these two sectors, and it simply creates unnecessary confusion and inconsistency. The committee supports the recommendation by the OPC that the Australian Government consider a systematic examination of both the IPPs and the NPPs with a view to developing a single set of consistent principles to be applied to both the public and private sector. The committee considers that the development of such principles could be undertaken by the ALRC as part of the review proposed in recommendations 1 and 2. However, the committee considers that it is crucial to ensure that there is no lowering of the standards currently applied by the IPPS and NPPs.

Recommendation 4

7.9 The committee recommends the development of a single set of privacy principles to replace both the National Privacy Principles and Information Privacy Principles, in order to achieve consistency of privacy regulation between the private and public sectors. These principles could be developed as part of the review by the Australian Law Reform Commission, as proposed in recommendations 1 and 2.

Emerging technologies

7.10 The committee is particularly concerned that the Privacy Act is simply not keeping up with the privacy challenges posed by new and emerging technologies. While the Privacy Act may have been an appropriate mechanism to respond to the technologies of the 1970s and 1980s, technology has moved at a rapid pace in the past few decades, and the Privacy Act has not been updated accordingly. The committee considers that the introduction of other legislation to deal with the emerging technologies, such as the *Spam Act 2003,* is a clear demonstration of the failure of the Privacy Act to adequately respond to new technologies.

7.11 The committee acknowledges calls for the Privacy Act to remain 'technology neutral'. Indeed, the committee considers that it is desirable for the Privacy Act to remain as 'technology neutral' as possible. However, the committee believes that it is possible update the Privacy Act in a 'technology neutral' way to reflect the technological changes that have occurred and to enable the Privacy Act to deal with these new technologies.

7.12 As mentioned above, the committee proposes that the ALRC review at recommendations 1 and 2 should examine ways to improve privacy regulation to improve its capacity to respond to emerging technologies. At the same time, the committee also agrees with some of the suggestions that were put forward during this inquiry. In particular, the committee considers that the Privacy Act should be amended to set out a statutory process for the conduct of privacy impact assessments in relation to new proposals which may have a significant impact on privacy. This assessment process could be a transparent and accountable way of ensuring that privacy concerns are addressed. The committee notes that privacy impact assessments are being conducted in relation to some new proposals such as biometric passports. However, the committee is concerned that these assessments are not being conducted in an open and transparent manner. The committee considers that such assessments need to involve full public consultation and should be occurring in a transparent and accountable manner. The committee considers that the details of this statutory privacy impact assessment process could be developed by the Australian Law Reform Commission as part of the review proposed in recommendations 1 and 2.

Recommendation 5

7.13 The committee recommends the Privacy Act be amended to include a statutory privacy impact assessment process to be conducted in relation to new projects or developments which may have a significant impact on the collection, use or matching of personal information.

7.14 The committee recognises suggestions that the definition of 'personal information' be updated to deal with new technologies and new methods of collecting information. In particular, the committee believes that consideration should be given to extending the definition to include information that enables an individual not only to be identified, but also contacted. This is also matter which should be examined by the review proposed at recommendations 1 and 2.

Recommendation 6

7.15 The committee recommends that the review by the Australian Law Reform Commission, as proposed in recommendations 1 and 2, examine the definition of 'personal information' in the *Privacy Act 1988*, and also any amendments to the definition which may reflect technological advances and international developments in privacy law.

Genetic information

7.16 In relation to the potential disclosure and discrimination use of genetic information, the committee endorses the recommendations of the report by the ALRC and NHMRC on the protection of human genetic information.[3] The committee notes that this report has been favourably received around the world, and indeed, established Australia as a world leader in relation to these issues. However, the committee considers the government's failure to date to respond to the report's recommendations is somewhat embarrassing. As a result, Australia is now starting to lag behind many other countries in dealing with this issue, to the possible detriment of many individual Australians.

7.17 The committee welcomes the recent budget announcement that funding will be provided for the establishment of a human genetics advisory committee as a principal committee of the NHMRC. The committee is disappointed that this does not fully match the ALRC and NHMRC's recommendations of an independent human genetic commission, but nevertheless welcomes any progress in addressing these issues and implementing the ALRC and NHMRC's report. However, the committee considers that the other recommendations in the ALRC and NHMRC's report should be implemented in full as a high priority.

Recommendation 7

7.18 The committee recommends that the Australian Government responds to, and implements, the recommendations of the *Essentially Yours* report into the protection of genetic information by the Australian Law Reform Commission and the Australian Health Ethics Committee of the National Health and Medical Research Council, as a high priority.

Other technologies

7.19 The committee notes the evidence received in relation to the privacy implications of smartcard technology, and that such technology can be either privacy enhancing or privacy invasive. The area of most immediate concern to the committee is the Medicare smartcard. The committee heard evidence of the lack of wider public consultation in relation to the privacy implications of the Medicare smartcard. Indeed, the committee is disturbed that it appears that key stakeholders were not consulted

3 ALRC and NHMRC, *Essentially Yours: Protection of Human Genetic Information in Australia,* ALRC 96, 2003, available at: http://www.austlii.edu.au/au/other/alrc/publications/reports/96/

prior to the introductory trial of the Medicare smartcard. The committee is also concerned about the potential for function creep in the use of the Medicare smartcard.

7.20 The committee is similarly concerned about the lack of public consultation, and indeed, the lack of publicly available information, in relation to the government's proposed national document verification service.

7.21 The committee also acknowledges concerns raised in submissions and evidence in relation to the privacy implications of biometric technology and the proposed biometric passports. The committee also notes the evidence of DFAT that a privacy impact assessment is being prepared in relation to the proposed biometric passports, in consultation with the OPC. However, once again, the committee is concerned that the privacy impact assessment does not appear to be being conducted in a particularly open or transparent manner.

7.22 The committee notes with concern the recent authorisation by the US FDA of human microchip implants. However, the committee was reassured to learn from relevant government departments that there are no similar proposals currently planned here in Australia. Nevertheless, the committee considers that this is an issue that has significant privacy implications, and that such microchip implants should be properly regulated here in Australia.

7.23 The committee also notes the extensive list of other technologies raised in submissions to the inquiry, including, but not limited to: RFID; spyware; location-based services; electronic messaging; and other telecommunications technology. The committee considers that the ALRC review should examine the privacy implications of these technologies, and whether appropriate regulatory measures are in place to ensure that privacy is adequately protected in relation to these technologies. Such regulatory measures should also be consistent and as technologically neutral as possible.

Recommendation 8

7.24 The committee recommends that the review by the Australian Law Reform Commission, as proposed in recommendations 1 and 2, include consideration of the privacy implications of new and emerging technologies with a view to ensuring that these technologies are subject to appropriate privacy regulation.

7.25 The committee notes in particular the recommendations of the OPC to address the issue of inconsistency between the Privacy Act and the Telecommunications Act. However, the committee considers that further measures could be taken, and therefore recommends that the ALRC review include a detailed examination of the interaction between the Privacy Act and the Telecommunications Act. This should include consideration of measures to reduce any inconsistency between these pieces of legislation and to ensure that privacy is adequately protected in the telecommunications area.

Recommendation 9

7.26 The committee recommends that the review by the Australian Law Reform Commission, as proposed in recommendations 1 and 2, consider the interaction of the *Privacy Act 1988* and the *Telecommunications Act 1997* with a view to recommending measures to reduce inconsistency between these pieces of legislation and to ensure that privacy is adequately protected in the telecommunications area.

Private sector provisions

7.27 The committee notes and endorses the findings and recommendations made by the OPC in its review of the private sector provisions of the Privacy Act. However, the committee considers that the OPC could have gone further in many of its recommendations. Further, the committee disagrees with the Privacy Commissioner's conclusions that the private sector provisions are 'working well'. Nevertheless, the committee recommends that the Australian Government responds to, and implements, the recommendations of OPC review as a high priority.

Recommendation 10

7.28 The committee recommends that the Australian Government responds to, and implements, the recommendations of the review of the private sector provisions by Office of the Privacy Commissioner as a high priority.

Exemptions

7.29 However, the committee notes that the OPC review's terms of reference were limited by the Attorney-General. The OPC review therefore failed to consider a number of relevant, and problematic, aspects of the private sector provisions, such as the exemptions for employee records and for political acts and practices. Hence, the committee repeats the need for the comprehensive review of the Privacy Act as proposed at recommendations 1 and 2.

7.30 In particular, the committee is concerned that the many exemptions under the Privacy Act are undermining the operation of the Privacy Act and adding to the problem of inconsistency across jurisdictions and sectors. Of particular concern to the committee are the small business exemption, employee records exemption and the political acts and practices exemption. The committee considers that a wider range of activities should be protected under the Privacy Act 1988, and is not convinced of the need for such broad exemptions.

Recommendation 11

7.31 The committee recommends that the review by the Australian Law Reform Commission, as proposed at recommendations 1 and 2, examine the operation of, and need for, the exemptions under the Privacy Act 1988, particularly in relation to political acts and practices.

Small business

7.32 The committee recognises that the Office of the Privacy Commissioner made a number of recommendations to address concerns about the small business exemption, including modifying the definition of small business so that it is based on the number of employees, rather than annual turnover. However, the committee is concerned that regulating some small businesses, such as in the areas of tenancy databases and telecommunications, but not others, will simply add to the complexity of the legislation. Indeed, the committee questions the need to retain the small business exemption at all. The committee recognises the evidence of organisations such EFA and APF that the exemption is too broad and too complex. In particular the committee notes that evidence of EFA that 'privacy rights do not disappear just because a consumer happens to be dealing with a small company.'[4] Similarly, the APF pointed out that some of the 'most privacy intrusive activities are carried out by very small companies and even sole traders.'[5]

7.33 Further, the committee considers that protecting the privacy of personal information also makes good commercial sense for all businesses, large and small. The committee notes that the privacy regimes of other jurisdictions, such as New Zealand, operate effectively without any small business exemption. Finally, the committee received evidence that the small business exemption is one of the key outstanding issues in negotiations with the European Union for recognition of Australia's privacy laws under the EU Data Protection Directive. Therefore, notwithstanding the proposed ALRC review, the committee recommends that the small business exemption be removed altogether from the Privacy Act.

Recommendation 12

7.34 The committee recommends that the small business exemption be removed from the *Privacy Act 1988*.

Employee records

7.35 In relation to the employee records exemption, the committee notes that a review of the employee records exemption was being undertaken by the Attorney-General's Department and the Department of Employment, Workplace Relations and Small Business. Indeed, this was the justification for excluding that exemption from the OPC's review of the private sector provisions. However, the progress of the review of the employee records exemption is unclear. The committee is disappointed at the slow progress of this review, and considers that this review should be finalised, and the results released, as a matter of urgency.

7.36 In any case, the committee notes with concern the evidence received that current workplace relations legislation does not adequately protect privacy in the

4 *Submission 17*, p. 34.

5 *Submission 32*, p. 14.

workplace. The committee agrees with the evidence of the Australian Law Reform Commission that the most appropriate place to protect employee privacy is in the Privacy Act, not workplace relations legislation. The committee also notes that state governments are acting to fill the legislative gaps by regulating workplace surveillance, but is concerned that this will only add to problems of inconsistency and fragmentation. The committee considers that employee records deserve appropriate and adequate privacy protection, and therefore recommends that the Privacy Act be amended to cover employee records.

Recommendation 13

7.37 The committee recommends that the privacy of employee records be protected under the *Privacy Act 1988*.

Recommendation 14

7.38 The committee recommends that the review by the Australian Law Reform Commission, as proposed at recommendations 1 and 2, should examine the precise mechanisms under the Privacy Act to best protect employee records.

Direct marketing

7.39 The committee again supports the recommendations of the OPC review in relation to direct marketing, particularly the proposal to amend the Privacy Act to require an organisation to take reasonable steps, on request, to advise an individual where it acquired the individual's personal information.[6] The committee also supports that the establishment of a national 'Do Not Contact' register. However, the committee suggests that the ALRC review proposed at recommendations 1 and 2 also consider the possibility of an 'opt in' regime for direct marketing in line with the *Spam Act 2003*.

Recommendation 15

7.40 The committee recommends that the review by the Australian Law Reform Commission, as proposed at recommendations 1 and 2, consider the possibility of an 'opt in' regime for direct marketing in line with the *Spam Act 2003*.

Adequacy for the purposes of the European Union

7.41 The committee notes that the EU still has not recognised Australia's Privacy Act as 'adequate' for the purposes of the EU Data Protection Directive. Notwithstanding the evidence that this has not had a significant impact on businesses trading with the EU, the committee considers it desirable for Australia's privacy laws to be recognised by the EU. The committee suggests that the issue of EU adequacy be considered by the ALRC review proposed at recommendations 1 and 2.

---

6 OPC review, Recommendation 24.

Recommendation 16

7.42 The committee recommends that the review by the Australian Law Reform Commission, as proposed at recommendations 1 and 2, examine measures that could be taken to assist recognition of Australia's privacy laws under the European Union Data Protection Directive.

Other aspects of the private sector provisions

7.43 The committee notes other suggestions made during its inquiry for other specific amendments to the Privacy Act and particularly NPPs. The committee recognises that many of these suggestions have merit. However, given the committee's recommendation of an ALRC review, and that the NPPs and IPPs should be merged, the committee makes no further recommendations for amendments, but rather proposes that these issues be considered as part of the review at recommendations 1 and 2, and in particular in the development of a single set of privacy principles as set out in recommendation 4 above.

Other issues

Credit reporting

7.44 The committee acknowledges the concerns raised by consumer advocates and groups in respect of the credit reporting regime established by Part IIIA of the Privacy Act. However, the committee does not see any need for review or reform of Part IIIA at this time. As noted in this report, action is being taken by industry to enhance data quality and to improve consumer engagement, including the development of better dispute resolution mechanisms.

7.45 However, the committee does consider that government action is required to maintain community confidence in integrity of the credit reporting regime. As Australia's largest credit reporting agency acknowledged, retaining the trust of individual consumers and the community at large is fundamental to credit reporting agencies' 'social licence to operate'.[7] The principal means of generating and maintaining that trust is through the effective enforcement of statutory privacy principles and rights. Yet evidence presented to the committee indicates that industry and consumers share concerns that regulatory oversight in the area of credit reporting is lacking. There is a view that, unless the OPC is provided with greater resources to take enforcement action and then prioritises enforcement action, the legislation will remain ineffective. The committee's position – explained below – is that the government must provide additional funding to the OPC as a matter of some urgency.

7.46 The committee sees no justification for the introduction of positive credit reporting in Australia. Moreover, the experience with the current range of credit information has shown that industry has not run the existing credit reporting system as

7 Baycorp Advantage, *Submission 43*, p. 5.

well as would be expected and it is apparent that injustice can prevail. As mentioned elsewhere in this report, positive reporting is also rejected on the basis that it would magnify the problems associated the accuracy and integrity of the current credit reporting system. The privacy and security risks associated with the existence of large private sector databases containing detailed information on millions of people are of major concern. For these reasons, the Committee's view is that positive reporting not be introduced

Recommendation 17

7.47 The Committee recommends that the Privacy Act not be amended to allow the introduction of positive credit reporting in Australia.

Health information and medical research

7.48 The committee notes evidence pointing to an urgent need for privacy laws relating to health information and medical research to be made uniform across the Australian jurisdictions. The committee accepts the view put by witnesses that the current arrangements are a failure of good government and inimical to the interests of health providers, researchers and patients in Australia. To this end, it urges the government to act on the recommendations made by the OPC in its review of the private sector provisions of the Privacy Act, especially the recommendations that a wider review of that Act be conducted and that the National Health Privacy Code be implemented as a schedule to that Act. Of particular concern to the committee is the evidence that the current privacy rules are hindering important medical research of potential benefit to all Australians.

Recommendation 18

7.49 The Committee recommends that the Australian Government, as part of a wider review of the Privacy Act, determine, with appropriate consultation and public debate, what is the appropriate balance between facilitating medical research for public benefit and individual privacy and the right of consent.

Responding to overseas emergencies

7.50 The committee acknowledges concerns raised by the ARC and DFAT in relation to impediments under the Privacy Act to information sharing in emergency situations. The committee notes that the OPC review made a number of recommendations to address this situation in relation to the private sector provisions. The committee therefore again urges the Australian Government to implement the recommendations of the OPC review as a matter of priority. The committee also suggests that the government ensure that it also addresses any impediments under the Privacy Act to information sharing between government agencies in such emergency situations.

Use of the Privacy Act as a means to avoid accountability and transparency

7.51 The committee acknowledges concerns about the use of the Privacy Act as a means to avoid accountability and transparency. The use of the Privacy Act as a 'shield' to justify privacy-invasive proposals and reassure the public is particularly concerning to the committee in light of the evidence received that the Privacy Act is actually not effective in protecting Australians' privacy. The committee hopes that other reforms recommended by the committee, and the OPC review, may improve this situation. In particular, the committee considers that increasing the resourcing available to the OPC, as recommended below, should help to alleviate this problem, particularly if some of those resources are directed to increasing awareness and understanding of privacy rights and obligations. The committee also sees merit in that the APF's suggestion of empowering the Privacy Commissioner to issue 'corrective statements', to be published at the expense of the organisation involved in the misrepresentation of the Privacy Act.

Law Enforcement Issues

7.52 The committee notes concerns raised by the AFP about problems encountered accessing information from organisations subject to the NPPs in relation to law enforcement issues. The committee supports the OPC's recommendation on this issue that it will develop practical guidance to assist private sector organisations to better understand their obligations under the Privacy Act in the context of law enforcement activities. However, the committee also considers that the Australian Government should examine additional mechanisms which may resolve this problem, such as the AFP's suggestion of the use of 'notices to produce'.

Resourcing and powers of the Office of the Privacy Commissioner

7.53 The committee acknowledges the considerable evidence received in the course of the inquiry which points to a serious lack of resourcing and inadequate powers of the OPC. In relation to resourcing issues, the committee is concerned that lack of funding is inhibiting the OPC from exercising its functions to full effect. In particular, the committee is mindful that, due to resource constraints, the OPC appears to be forced to concentrate on dealing with individual consumer complaints, at the expense of other important strategic functions.

7.54 Several findings and recommendations made by the OPC in its review of the private sector provisions relate to resourcing and powers of the OPC. As noted in paragraph 7.27, the committee endorses the findings and recommendations made by the OPC in its review, however the OPC could have gone much further in many of its recommendations. While the committee encourages the Australian Government to implement the recommendations of the OPC review as a matter of priority,[8] the committee considers that, in relation to resourcing of the OPC, an immediate

8 See OPC review, Recommendation 10, para 7.78.

allocation of additional funding is required to enable the OPC to more efficiently and effectively fulfil its mandate.

7.55 The committee also notes concerns raised by the APF in relation to the OPC review's recommendation that there be discretion not to investigate complaints where the harm to individuals is minimal and there is no public interest in pursuing the matter. The committee urges the Australian Government to consider carefully the various implications of such an approach.

7.56 Further, the committee considers that the OPC review's recommendations relating to powers of the Privacy Commissioner should be implemented as soon as possible.[9] In particular, the committee urges the introduction of private sector auditing powers for the OPC.

Recommendation 19

7.57 The committee recommends that the Australian Government provide an immediate allocation of additional funding to the Office of the Privacy Commissioner to enable it to more efficiently and effectively fulfil its mandate and to ensure genuine and systemic improvements to its operation, both now and into the future.

Senator the Hon Nick Bolkus

Chair

9 See OPC review, Recommendation 10, para 7.78.

ADDITIONAL COMMENTS BY SENATOR NATASHA STOTT DESPOJA

1.1 I feel compelled to add some additional comments to the Committee's observations regarding the exemption for political acts and practices in the Privacy Act.

1.2 In considering whether there is any justification for this exemption, it is important to examine its practical effect. As the Committee notes, the Government has sought to justify this exemption on the basis that it fosters freedom of political communication and enhances the democratic process. However, the evidence suggests that the opposite is the case.

1.3 This exemption has allowed some political parties to develop extensive databases, containing information about their constituents, the most notable of which are the Coalition's database, *Feedback*, and the Australian Labor Party's database, *Electrac*.

1.4 The practical operation of these databases has been described in detail by Peter Van Onselen and Wayne Errington in their article, "Electoral Databases: Big Brother or Democracy Unbound?"[1]:

> The design and operation of electoral databases is fairly simple. Access to commercially available information, the Australian Electoral Commissioner (AEC) data and the telephone directory provides the raw material of names and addresses of constituents. That is where the hard work begins. The purpose of these databases is to provide parties with information about the policy and voting preferences of individual voters, and to collate this information in ways useful to political campaigning[2].

1.5 Van Onselen and Errington go on to explain that the databases are enhanced in two different ways, the first of which involves 'tagging' individual voters according to their voting information, party affiliation, history of donations and ethnic identity. These tags are:

> based on information gathered through contact with the electorate office, local newspaper coverage (letters to the editor providing good information about issues of interest to particular voters), door-knocking and telephone canvassing[3].

---

[1] *Australian Journal of Political Science, Vol. 39, No.2, July 2004, p. 349-366.*

[2] Van Onselen and Errington, p. 353.

[3] Van Onselen and Errington, p. 353.

1.6 The second way of adding to the databases is to collect detailed information when constituents contact the office of a parliamentarian or candidate. Office staff are trained to log the details of all telephone conversations, correspondence and face-to-face meetings into the database.

1.7 A particular concern relating to the collection of information by this means is that it blurs the line between members of parliament as holders of public office on the one hand, and as members of a political party on the other. Constituents may well need to seek the assistance of their local member and, in doing so, they may need to disclose detailed information about their personal life, welfare benefits, employment, or involvement in community groups. Questions arise as to whether such information, which has been provided to a public office holder for the purpose of seeking assistance, should then be entered onto a database designed to advance the interests of a political party.

1.8 There are a number of additional concerns relating to the operation of these databases. The first relates to the widespread practice of providing training courses on database operation under the Parliamentary Entitlements Act, which amounts to the use of public resources for party political gain.

1.9 Secondly, the databases foster a preoccupation with swinging voters at the expense of other constituents. While this understandable in an electoral context, it raises questions about the democratic process, more generally. As Van Onselen and Errington note, the primary purpose of these databases is to identify and influence swinging voters. They ask:

> Do databases contribute to the marginalisation of large numbers of voters on the basis that they can be identified as strongly supporting a political party? Does the targeting of campaigns towards swinging voters skew public policy towards the wants of a tiny minority of the electorate…? These questions strike at the very heart of representative democracy.[4]

1.10 Finally, constituents have no right to access the information held about them or to correct that information if it is inaccurate. This is particularly concerning given that these databases contain information about the political views of constituents. Some of the means by which information is collected and entered onto the databases raise serious questions about the accuracy of the information. However, the other obvious point to make is that political views are often fluid and can change over time.

1.11 With these concerns in mind, the stated justification for the exemption from the Privacy Act – namely, that it is intended to encourage freedom of political communication and enhance the political process – rings rather hollow.

1.12 On the contrary, the unregulated operation of political databases has the potential to diminish public confidence in the democratic process, discourage

[4] Van Onselen and Errington, p. 361.

constituents from contacting their local Member of Parliament and distorting the political process by skewing it further in favour of swinging voters.

1.13 While it is true that these databases "would be much less effective were political parties not exempted from the Privacy Act"[5], it is also clear that they could continue to operate in a more regulated fashion, should the exemption be abolished. Perhaps the most significant difference would be that individual Australians would, for the first time, have a right to access the information held about them by political parties and to correct any information that might be inaccurate.

Senator Natasha Stott Despoja

Australian Democrats

[5] Van Onselen and Errington, p. 349.

APPENDIX 1

SUBMISSIONS RECEIVED

1	Real Estate Institute of Australia
2	The Cancer Council New South Wales
3	Fundraising Institute Australia
4	Bio21 Australia
5	National Serology Reference Laboratory
6	ANZ
7	Mr Ian Cunliffe
8	Australian Press Council
9	Australian Medical Association Limited
9a	Australian Medical Association Limited
10	Confidential
11	Lockstep Consulting Pty Ltd
12	Anti Discrimination Board of New South Wales
13	Queensland Institute of Medical Research
14	Sony Business Solutions
15	Australian Consumers' Association
16	Australian Entertainment Industry Association
17	Electronic Frontiers Australia Inc
17A	Electronic Frontiers Australia Inc
18	Australian Law Reform Commission
19	Ms Mary Lander
20	National Health and Medical Research Council

21	Caroline Chisholm Centre for Health Ethics
22	Dr Anthony G Place
23	Mr David Travis
24	Centre for Law and Genetics
25	Australia Chamber of Commerce Industry
26	Australian Electrical and Electronic Manufacturers' Association Limited
27	Australian Institute of Health and Welfare
28	Mr Roger Clarke
29	Care Leavers of Australia Network
30	Festival of Light Australia
31	Legal Aid Queensland
32	Australian Privacy Foundation
32a	Australian Privacy Foundation
32b	Australian Privacy Foundation
33	Office of the Victorian Privacy Commissioner
33a	Office of the Victorian Privacy Commissioner
34	Department of Health and Ageing
34a	Department of Health and Ageing
35	Consumer Credit Legal Centre (NSW)
36	Credit Union Services Corporation (Australia) Limited
37	Law Institute of Victoria
37a	Law Institute of Victoria
38	Australian Direct Marketing Association
39	Department of Foreign Affairs and Trade
40	Consumers' Federation of Australia

41	Australian Communication Exchange
42	Australian Federal Police
42a	Australian Federal Police
43	Baycorp Advantage
43a	Baycorp Advantage
44	Australian Red Cross
44a	Australian Red Cross
45	Department of Family and Community Services
46	Ms Judy Gill
47	Hitwise
48	Office of the Privacy Commissioner
49	Attorney-General's Department

APPENDIX 2

WITNESSES WHO APPEARED BEFORE THE COMMITTEE

Melbourne, Friday, 22 April 2005

Office of the Victorian Privacy Commissioner

Mr Paul Chadwick, Victorian Privacy Commissioner

Law Institute of Victoria

Mr William O'Shea, Council Member, Past President

Ms Joanne Kummrow, Solicitor, Administrative Law and Human Rights Section

Mr Nihal Samararatna, Member

Legal Aid Queensland (by teleconference)

Ms Loretta Kreet, Solicitor, Civil Justice (Consumer Protection) Team

Australian Red Cross

Mr Robert Tickner, Secretary General (Chief Executive Officer)

Mr Noel Clement, General Manager, Domestic Operations (National Programs)

Mr Greg Heesom, National Manager, International Humanitarian Law

Electronic Frontiers Australia

Ms Irene Graham, Executive Director

Sydney, Thursday, 19 May 2005

Baycorp Advantage

Mr Andrew Want, Chief Executive Officer

Mr Chris Gration, Consultant

Ms Melissa Stratton, Group Privacy Adviser

Australian Privacy Foundation

Ms Anna Johnston, Chair

Mr David Vaile, Vice Chair

Australian Consumers' Association

Mr Charles Britton, Senior Policy Officer, IT and Communications

Australian Direct Marketing Association

Miss Jodie Sangster, Director, Legal and Regulatory Affairs

Australian Law Reform Commission

Professor David Weisbrot, President

Ms Carolyn Adams, Principal Legal Officer

Office of the Privacy Commissioner

Ms Karen Curtis, Privacy Commissioner

Mr Timothy Pilgrim, Deputy Privacy Commissioner

Attorney-General's Department

Ms Philippa Lynch, First Assistant Secretary, Information Law and Human Rights Division

Ms Janine Ward, Acting Assistant Secretary, Information Law Branch

Mr Colin Minihan, Principal Legal Officer, Information Law Branch, Private Sector Privacy

Canberra, Friday, 20 May 2005

Department of Foreign Affairs and Trade

Mr Rod Smith, First Assistant Secretary, Public Diplomacy, Consular and Passports Division

Mr Bob Nash, Assistant Secretary, Passports Branch

Mr Adrian White, Manager, Passports Act Review Team, Passports Branch

Ms Stacey Morgan, Executive Officer, Administrative and Domestic Law Section, Legal Branch

Centre for Law and Genetics (by teleconference)

Professor Donald Chalmers, Director

Dr Dianne Nicol, Senior Research Fellow

Australian Medical Association

Ms Pamela Burton, Legal Counsel

Ms Julia Nesbitt, Director, General Practice and E-health

National Health and Medical Research Council (NHMRC)

Professor David Hill, Member, NHMRC Research Committee, and Chair, NHMRC Working Committee on Privacy

Dr David Whiteman, Council Member, and Member, NHMRC Working Committee on Privacy

Professor Colin Thomson, NHMRC Consultant in Health Ethics

Mrs Cathy Clutton, Acting Executive Director, Centre for Health Advice, Policy and Ethics

Department of Health and Ageing

Ms Mary Murnane, Deputy Secretary

Ms Margaret Lyons, First Assistant Secretary, Health Services Improvement Branch

Dr Brian Richards, National Director, e-Health Implementation Group

Mr Mike McGrath, Legal Adviser

Australian Federal Police

Mr Trevor Van Dam, Chief Operating Officer

Federal Agent Peter Drennan, National Manager, Economic and Special Operations

Mr James Watson, Manager, Legal