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.