CHAPTER 3

EMERGING TECHNOLOGIES

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

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

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

In general

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

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

---

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

---

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

7 *Submission 28*, p. 1.

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

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

10 *Submission 15*, p. 1.

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

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

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

Technological neutrality

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

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

3.11 The APF supported this approach:

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

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

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

---

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

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

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

15 *Submission 32*, p. 10.

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

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

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

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

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

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

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

3.16 The LIV then gave the following examples:

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

---

16 *Submission 43*, p. 11.

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

18 *Submission 28*, p. 2.

19 *Submission 37*, p. 9.

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

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

Definition of 'personal information'

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

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

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

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

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

---

20 *Submission 37*, p. 9.

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

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

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

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

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

3.21 Ms Irene Graham from EFA explained:

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

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

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

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

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

---

25 *Submission 17*, p. 32.

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

27 *Submission 17*, p. 33.

28 *Submission 17A*, p. 5.

29 *Submission 17A*, p. 5.

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

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

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

Privacy impact assessments

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

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

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

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

3.27 The LIV continued:

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

---

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

33 *Submission 47*, p. 4.

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

35 *Submission 32*, p. 11.

36 *Submission 37*, pp 6-7.

37 *Submission 37*, p. 7.

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

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

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

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

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

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

---

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

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

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

41 OPC review, p. 256.

42 OPC review, p. 256.

OPC review

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

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

3.33 The OPC review also committed to issuing:

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

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

Smart cards and national identification schemes

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

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

43 OPC review, pp 239-257.

44 OPC review, Recommendation 69, p. 257.

45 OPC review, Recommendation 71, p. 257.

46 OPC review, Recommendation 73, p. 257.

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

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

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

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

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

---

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

48 *Submission 37*, p. 10.

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

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

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

52 *Submission 11*, p. 1.

53 *Submission 11*, p. 5.

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

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

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

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

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

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

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

---

54 *Submission 33*, p. 4.

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

56 *Submission 17*, p. 25.

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

58 *Submission 37*, p. 10.

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

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

Function creep and national ID schemes

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

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

3.44 EFA continued:

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

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

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

---

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

62 *Submission 17*, p. 19.

63 *Submission 17*, p. 19.

64 *Submission 17*, p. 20.

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

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

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

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

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

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

3.48 At the same time, the ACA acknowledged that:

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

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

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

---

67 *Submission 15*, p. 9.

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

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

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

71 *Submission 15*, pp 7-8.

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

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

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

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

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

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

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

72 *Submission 32*, p. 10.

73 *Submission 32*, p. 10.

74 *Submission 32*, p. 10.

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

76 *Submission 17*, pp 29-30.

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

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

3.54 The representative further stated that:

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

Medicare smartcard

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

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

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

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

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

---

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

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

80 *Submission 34*, pp 13-14.

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

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

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

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

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

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

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

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

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

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

---

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

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

86 *Submission 17*, p. 24.

87 *Submission 8*, p. 6.

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

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

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

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

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

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

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

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

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

89 *Submission 34B*, p. 2.

90 *Submission 34B*, p. 2.

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

92 *Submission 48*, p. 14.

93 *Submission 17*, p. 23.

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

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

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

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

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

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

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

Biometrics

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

---

95 *Submission 17*, p. 22.

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

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

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

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

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

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

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

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

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

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

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

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

---

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

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

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

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

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

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

108 *Submission 37*, p. 11.

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

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

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

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

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

Biometric Passports

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

---

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

111 *Submission 11*, p. 18.

112 *Submission 11*, p. 18.

113 *Submission 26*, p. 2.

114 *Submission 33*, p. 4.

115 *Submission 20*, p. 5.

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

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

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

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

3.78 The representative of DFAT elaborated on this:

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

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

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

---

118 *Submission 39*, p. 1.

119 *Submission 39*, p. 2.

120 *Submission 39*, p. 1.

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

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

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

124 *Submission 39*, p. 1.

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

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

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

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

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

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

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

---

125 *Submission 39*, p. 4.

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

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

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

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

130 *Submission 17*, p. 29.

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

132 *Submission 28*, p. 2.

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

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

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

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

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

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

3.89 A representative of DFAT responded to these concerns:

---

133 *Submission 17*, p. 27.

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

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

136 *Submission 15*, p. 12.

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

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

Draft Biometrics Privacy Code

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

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

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

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

---

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

139 See further www.biometricsinstitute.org

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

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

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

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

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

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

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

Genetic testing and discrimination

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

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

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

143 *Submission 15*, p. 2.

144 *Submission 15*, p. 11.

145 OPC review, Recommendation 73, p. 257.

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

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

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

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

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

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

---

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

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

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

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

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

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

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

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

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

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

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

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

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

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

---

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

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

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

156 *Submission 12*, p. 3.

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

158 *Submission 12*, p. 3.

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

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

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

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

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

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

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

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

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

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

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

3.107 Professor Weisbrot of the ALRC noted that:

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

---

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

163 *Submission 13*, p. 3.

164 *Submission 5*, p. 2.

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

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

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

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

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

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

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

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

---

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

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

168 *Submission 18*, p. 8.

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

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

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

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

Genetic discrimination

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

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

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

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

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

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

---

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

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

174 *Submission 2*, p. 4.

175 *Submission 2*, p. 3.

176 *Submission 2*, p. 4.

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

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

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

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

Response to the Essentially Yours report

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

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

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

---

179 *Submission 12*, p. 6.

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

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

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

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

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

3.119 The ALRC noted in its submission that:

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

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

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

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

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

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

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

---

184 *Submission 20*, p. 6.

185 *Submission 18*, p. 2.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

---

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

196 *Submission 34A*, p. 3.

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

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

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

Microchip implants and RFID technology

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

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

3.134 As the Office of the Victorian Privacy Commissioner observed:

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

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

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

---

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

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

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

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

203 *Submission 33A*, p. 2.

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

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

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

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

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

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

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

---

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

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

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

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

209 *Submission 20,* p. 6.

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

3.139 Mr Roger Clarke argued that:

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

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

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

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

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

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

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

---

210 *Submission 28*, p. 2.

211 *Submission 28*, p. 2.

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

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

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

215 *Submission 34*, pp 19-20.

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

RFID technology

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

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

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

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

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

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

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

---

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

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

218 *Submission 33A*, p. 2.

219 *Submission 15*, p. 4.

220 *Submission 15*, pp 4-5.

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

Other technologies and related issues

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

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

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

3.151 Mr Roger Clarke also pointed to:

---

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

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

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

224 *Submission 15*, pp 2-7.

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

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

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

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

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

3.153 The LIV also suggested that this inquiry should examine:

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

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

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

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

3.156 EFA explained further

---

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

228 *Submission 37*, p. 9.

229 *Submission 37*, p. 6.

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

231 *Submission 17*, pp 9-14.

232 *Submission 17*, p. 9.

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

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

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

233 *Submission 17*, p. 9.

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