Chapter 2

Australia's privacy framework

2.1 The Office of the Privacy Commissioner (OPC) submitted that 'the best approach to enhancing privacy online will be multi-faceted'[1] and outlined the components comprising the existing approach to protecting privacy in Australia, which include:

- the *Privacy Act 1988*;
- complaints mechanisms;
- industry self-regulation;
- education;
- privacy enhancing technology; and
- international cooperation.

2.2 Each of these mechanisms is discussed below with a focus on its protection of the privacy of Australians in the online context. Proposed changes to each mechanism are also discussed where relevant.

Legislation

2.3 The key piece of legislation relating to privacy in Australia is the *Privacy Act 1988*. The Privacy Act 'regulates the handling of personal information by most Australian and ACT government agencies, large private sector organisations and some small businesses'.[2]

2.4 The Privacy Act currently contains separate sets of 'privacy principles' for public sector agencies and private sector organisations—the Information Privacy Principles (IPPs) and National Privacy Principles (NPPs) respectively.[3] In essence, the principles set out standards for managing and using personal information including collection, use, disclosure, storage and destruction.

2.5 The Privacy Act also established the OPC, recently integrated into the Office of the Australian Information Commissioner (OAIC).[4]

2.6 The OPC submitted that:

> The Privacy Act provides a mechanism to support good personal information handling by government agencies and private sector

---

1 OPC, *Submission 16*, p. 10.

2 OPC, *Submission 16*, p. 10.

3 The NPPs, IPPs and proposed Australian Privacy Principles (APPs) are set out in Appendix 3.

4 *Privacy Act 1988*, Part IV.

> organisations and offers an avenue of redress for individuals that believe that their personal information has been misused.[5]

2.7 The OPC argued that one of the strengths of the Privacy Act is the fact that it uses 'principles' rather than 'prescriptive rules' which has provided a framework that is 'adequately flexible to respond to technological change'.[6] The OPC's submission gives the example of NPP 4.1 which requires private sector organisations to 'take reasonable steps to protect the personal information it holds…'.[7] What constitutes 'reasonable steps' will depend on the circumstances, including the development and availability of new technologies.

2.8 However, despite this inbuilt flexibility, the Australian Law Reform Commission's (ALRC) 2008 review of privacy law and practice in Australia resulted in a range of recommendations as to how the Privacy Act might be improved.[8] The OPC submitted:

> Since its enactment over 20 years ago, the Privacy Act has operated against a backdrop of significant change associated with the information age and the rise of the internet. To ensure the ongoing effectiveness of the Privacy Act in a rapidly evolving technological environment, considerable work has been done in recent years to review and reform the act. Most significantly, the Australian Law Reform Commission undertook a review of privacy—the largest review to date—and the government has provided a first stage response to that review.[9]

2.9 The ALRC's review also examined the role of telecommunications laws in protecting privacy in Australia, and 34 of the recommendations in its 2008 report dealt with the *Telecommunications Act 1997*, *Spam Act 2003* and *Do Not Call Register Act 2006*.[10] The government is yet to respond to these telecommunications-specific recommendations.[11]

2.10 The government has announced that it intends to respond to the ALRC's recommendations in two stages,[12] and has released the first stage of its response.[13] The

---

5 OPC, *Submission 16*, p. 8.

6 OPC, *Submission 16*, p. 10.

7 OPC, *Submission 16*, p. 10.

8 ALRC, *For Your Information: Australian Privacy Law and Practice*, Report No 108, 2008, www.alrc.gov.au/publications/report-108 (accessed 18 January 2011).

9 Mr Timothy Pilgrim, Australian Privacy Commissioner, *Committee Hansard*, 29 October 2010, p. 17.

10 Mr Duncan McIntyre, Assistant Secretary, Consumer Policy and Post, Department of Broadband, Communications and the Digital Economy (DBCDE), *Committee Hansard*, 29 October 2010, pp 83–84.

11 Mr Duncan McIntyre, Assistant Secretary, Consumer Policy and Post, DBCDE, *Committee Hansard*, 29 October 2010, pp 83–84.

12 Department of the Prime Minister and Cabinet, 'Privacy Reforms', www.dpmc.gov.au/privacy/reforms.cfm (accessed 14 December 2010).

government has also released an exposure draft of amendments to the Privacy Act, which is being considered by the Senate Finance and Public Administration Legislation Committee.[14] The key purpose of the exposure draft is to replace the NPPs and IPPs with uniform principles which apply to both the public and private sector—to be called the Australian Privacy Principles (APPs). This reform follows a recommendation by the ALRC and is intended to 'reduce confusion, overlap and inconsistency'.[15]

2.11 The OPC's submission argues that the government's proposed amendments to the privacy principles 'will enhance the operation of the Privacy Act, ensuring it remains effective in the face of continuing technological change'.[16]

2.12 Google agreed that the government's proposed amendments will strengthen the Act:

> We think that the draft privacy legislation currently before the finance and public administration committee is based on a strong principles based framework that has the flexibility to respond to further developments in technology. Another key element of the privacy framework is to have an independent and effective privacy regulator, which is what we believe we have.[17]

2.13 However, other organisations are concerned that the introduction of uniform principles for the public and private sector may weaken privacy protection in Australia. For example, Ms King-Siem, Vice-President, Liberty Victoria noted:

> Having the IPPs and the NPPs originally was a convenient way for the government to introduce regulation of the private sector and take a far softer approach between the private sector and the public sector...there is concern that the APPs are taking a slightly more watered down approach than they could otherwise.[18]

2.14 While many of the proposed amendments to privacy and telecommunications legislation in Australia are relevant to this inquiry, the committee has chosen not to examine the exposure draft in detail given that it is already the subject of another

---

13 Senator the Hon Joe Ludwig, Cabinet Secretary, *Enhancing National Privacy Protection: Australian Government First Stage Response to the Australian Law Reform Commission Report 108*, October 2009.

14 Senate Finance and Public Administration Legislation Committee, Inquiry into Exposure Drafts of Australian Privacy Amendment Legislation, www.aph.gov.au/Senate/committee/fapa_ctte/priv_exp_drafts/index.htm, (accessed 22 October 2010).

15 OPC, *Submission 16*, p. 11.

16 OPC, *Submission 16*, p. 9.

17 Mr Iarla Flynn, Head of Public Policy and Government Affairs, Google Australia Pty Ltd, *Committee Hansard*, 29 October 2010, p. 2.

18 Ms Georgia King-Siem, Vice-President, Victorian Council for Civil Liberties (Liberty Victoria), *Committee Hansard*, 1 December 2010, p. 20.

Senate committee inquiry. Certain aspects of the proposed legislation, relevant to online privacy specifically, are considered throughout this report, but the committee has not conducted an extensive review of the legislation or proposed amendments as a whole.

2.15 Most States and Territories have legislative privacy protections, with the exceptions of South Australia and Western Australia.[19] Victoria and the ACT also have a right to privacy included in their *Charter of Human Rights and Responsibilities Act 2006* (Vic) and *Human Rights Act 2004* (ACT) respectively.

2.16 However, the OPC noted that:

> Legislation alone is not sufficient to ensure the protection of privacy for Australians online. One reason for this is that domestic laws will not always have jurisdiction in the transnational space of the internet.[20]

Complaints mechanisms

2.17 The Australian Communications Consumer Action Network (ACCAN) submitted that 'complaints are a vital element in privacy protection—indeed, the entire system of privacy protection in the communications sector is built on the receipt and management of complaints'.[21]

2.18 ACCAN recently commissioned the Cyberspace Law and Policy Centre to conduct a research project into privacy complaints in the Australian communications sector which compared complaints made to the OPC, the Australian Communications and Media Authority (ACMA) and the Telecommunications Industry Ombudsman (TIO). Each organisation is responsible for privacy complaints made under different circumstances: the OPC deals with general privacy complaints, and telemarketing and internet related complaints; ACMA deals with spam and do-not-call complaints, plus a small number of general privacy complaints; and the TIO deals with general privacy complaints and internet related complaints.[22]

2.19 The study found vast differences in the number of complaints made to each organisation. In 2009 the ACMA received a total of 16 014 privacy complaints, the TIO received 4942, and the OPC 113.[23] ACCAN acknowledges that the ACMA's jurisdiction over do-not-call register and spam complaints means that it will always receive the highest number of complaints. However, ACCAN noted that the number

---

19 Victorian Privacy Commissioner, *Submission 13*, p. 2.

20 OPC, *Submission 16*, p. 9.

21 ACCAN, *Submission 11*, p. 3.

22 ACCAN, *Submission 11*, pp 3–4; Cyberspace Law and Policy Centre, UNSW, *Communications privacy complaints: In search of the right path*, 2010, p. 6, at www.cyberlawcentre.org/privacy/ACCAN_Complaints_Report/report.pdf (accessed 23 December 2010).

23 Cyberspace Law and Policy Centre, UNSW, *Communications privacy complaints: In search of the right path*, 2010, p. 8.

of complaints to the OPC—the major national privacy regulator—is concerningly low.[24]

2.20 The study also found that the average time for dispute resolution was 5 days for the ACMA, 10 days for the TIO and 180 days for the OPC.[25] While noting that 'a small delay is to be expected at the OPC as they have a strong focus on conciliation and some of their matters may be more complex', ACCAN submitted that 'no consumer should be waiting 6 months to have a privacy complaint in the communications sector resolved'.[26]

2.21 In this respect, Ms Teresa Corbin, CEO, ACCAN, emphasised:

> I think it is also important to acknowledge that all these agencies have very different ways of approaching these complaints. For example, one of the reasons the Privacy Commissioner takes longer to deal with these complaints is that they conduct an investigation and conciliation. That is a very different process to an investigation and then making a decision awarding an outcome, which is what the ACMA and the TIO both do, because their powers allow it.[27]

2.22 While the report was generally very positive about the ACMA's complaints handling, the ACMA similarly argued that it is important that the distinct roles of each privacy complaints-handling agency is considered when examining the disparity in resolution timeframes:

> I would just like to draw the distinction that each of us [the ACMA, the OPC and the TIO], when we are working in regulatory spheres, have different responsibilities and different issues that we look at. Some investigations are quite straightforward. Things like the Do Not Call Register are quite straightforward: either somebody is on the register or not on the register or has given consent or not. The Privacy Commissioner, I would expect, would have quite complex investigations from time to time and they always take a bit longer. So, while we welcomed ACCAN's research, as we always do, we felt that there were some areas in there that could have been fleshed out a bit more to point out the differences in people's regulatory responsibilities.[28]

2.23 However, the study also found a range of other issues with the existing privacy complaints structure. For example, the study found that the three complaints pathways also result in disparate outcomes for consumers. ACCAN submitted that while the OPC is able to deliver a complainant compensation or an apology, it will not

---

24 ACCAN, *Submission 11*, pp 4–5.

25 Cyberspace Law and Policy Centre, UNSW, *Communications privacy complaints: In search of the right path*, 2010, p. 10.

26 ACCAN, *Submission 11*, p. 5.

27 Ms Teresa Corbin, CEO, Australian Communications Consumer Action Network (ACCAN) *Committee Hansard*, 29 October 2010, pp 44–45.

28 Ms Nerida O'Loughlin, General Manager, Digital Economy Division, Australian Communications and Media Authority, *Committee Hansard*, 1 December 2010, p. 58.

provide a prompt solution such as immediate correction or removal of personal data. The ACMA is able to deliver prompt corrections, and can also undertake enforcement action, such as fines, but cannot order compensation to a complainant. The TIO can also deliver prompt action and limited enforcement actions.[29] ACCAN argued that this situation is unacceptable and submitted that:

> *Any* privacy complaint in the communications sector lodged with *any* complaints body should be able to achieve all of the outcomes that are desirable in a best practice regulatory environment.[30]

2.24 ACCAN submitted that the information given to consumers about likely resolution times is 'fairly ad hoc and inconsistent', and recommended that this information be made clear to consumers so that they can choose the best avenue to resolve their complaint.[31]

2.25 ACCAN also raised concerns about the accessibility of complaints mechanisms to disadvantaged and vulnerable consumers, but noted that the study was unable to draw conclusions about this issue as no data was kept on the profile of complainants.[32] The CEO of ACCAN, Ms Corbin, stated:

> Obviously, those who are most disadvantaged and vulnerable in our community are also going to be most disadvantaged and vulnerable when it comes to privacy, because a lot of the privacy protection—not waiving rights—revolves around people having high levels of literacy. Clearly, in some of those vulnerable and disadvantaged groups they may well still be using plenty of online services but not necessarily reading everything that goes across the screen. It could well be that they are just using lots of other cues—for example, icons, pictures and video. So, yes, it is a concern and something that we need to do some more work on.[33]

2.26 The Cyberspace Law and Policy Centre made a number of recommendations in its report based on these findings, including: more coordination between the three agencies; consistent messages to consumers and industry; and providing each agency with a full range of regulatory tools.[34]

2.27 Ms Corban informed the committee that ACCAN has approached the OPC with the aim of addressing the issues raised in the study:

> We are hoping it is an opportunity to improve the situation. That is how we have approached the Privacy Commission, although they obviously were not too pleased about our report. We have suggested that, in our dialogue from now on, we actually focus on: why is this the case, how can it be

29 ACCAN, *Submission 11*, p. 6.

30 ACCAN, *Submission 11*, p. 7, emphasis in original.

31 ACCAN, *Submission 11*, p. 6.

32 ACCAN, *Submission 11*, p. 6.

33 Ms Teresa Corbin, CEO, ACCAN, *Committee Hansard*, 29 October 2010, p. 49.

34 Cyberspace Law and Policy Centre, UNSW, *Communications privacy complaints: In search of the right path*, 2010, p. 25.

> improved? Also, perhaps it cannot be taken to be exactly the same as the TIO or the ACMA, but how can we actually reduce that time? Or do we need to get more resources to that body? Maybe the new resources that are available because of the information commission will assist there.[35]

2.28 ACCAN has also suggested that the OPC provide more information to consumers about their options, for example by publishing their decisions so that:

> ...then there would be a better awareness of why it takes longer to get an apology than to trigger that enforcement notice. I think there is room for some further explanation from the Privacy Commissioner, but I think there is also some room for improvement, even within the existing powers and structure that they have.[36]

2.29 In response to the Cyberspace Law and Policy Centre's report, the OPC commented:

> The report does not distinguish between the types of privacy complaints received by the Privacy Commissioner, the Telecommunications Industry Ombudsman and the Australian Media and Communications Authority. The Privacy Commissioner can only deal with matters that can be treated as complaints under the *Privacy Act 1988* (Cth). A number of these telecommunications privacy complaints are about credit reporting, which by their nature are complex and generally require detailed investigation.
>
> Nor is it appropriate, without qualification, to compare the investigation times required for complex complaints under the *Privacy Act 1988* with those complaints received under the Spam Act or the Do Not Call Register Act... The Office focuses on working cooperatively with complainants and respondents to resolve complaints through conciliation by achieving outcomes such as apologies, improved business processes, and compensation if appropriate. This negotiation process necessarily takes time.[37]

Committee comment

2.30 The committee urges the government to consider the report of the Cyberspace Law and Policy Centre, and respond to the recommendations made therein, and by ACCAN in response to the report. Specifically, the committee recommends that the government focus on ways to address the inconsistencies in privacy complaint-handling agencies' investigative tools, the lack of coordination between the agencies, and issues identified by the Cyberspace Law and Policy Centre and ACCAN with respect to providing consistent, clear messages to consumers about their options.

---

35 Ms Teresa Corbin, CEO, ACCAN, *Committee Hansard*, 29 October 2010, p. 50.

36 Ms Teresa Corbin, CEO, ACCAN, *Committee Hansard*, 29 October 2010, p. 50.

37 M. Hummerston, Assistant Privacy Commissioner, media release, 14 September 2010.

Recommendation 1

2.31 The committee recommends that the government consider and respond to the recommendations in the Cyberspace Law and Policy Centre's report: *Communications privacy complaints: In search of the right path*, and recommendations from the Australian Communications Consumer Action Network arising from that report.

Industry self-regulation

2.32 Currently, because many organisations managing browsers, social networking sites, and other web 2.0 sites operate outside of the scope of the Privacy Act for various reasons,[38] the privacy of Australians online appears to be largely dependent on the policies and practices of the online sites they use.

2.33 For those Australian organisations that operate outside of the Privacy Act, while the OPC may issue guidelines for best practice in information handling and privacy policy, it is currently up to individual organisations to implement these policies. Overseas based organisations may be required to comply with privacy laws in the jurisdiction in which they are based.

2.34 With respect to organisations bound by the Privacy Act, the Act currently provides that organisations may develop industry codes with at least equivalent protections to the NPPs, which organisations within the industry may consent to be bound by. Codes must be approved by the Commissioner.[39] The government proposes to extend the powers of the Privacy Commissioner to request the development of an industry privacy code where the Commissioner considers it would be in the public interest for such a code to be developed.[40]

2.35 The government has also proposed that if an adequate code is not developed following such a request by the Commissioner, the Commissioner should have the power to develop and impose such a code following consultation with stakeholders.[41]

2.36 The OPC has suggested that binding codes may be appropriate:

> …for certain types of data-matching where there may be heightened privacy risks, for specific notice requirements for new technologies, and to allow standards developed by industry bodies to be given lawful effect.[42]

2.37 The OPC supports the government's proposal to expand its powers in this way, submitting that:

---

38 Predominantly because the organisations are based overseas or because they are Australian businesses subject to the small business exemption under the Privacy Act. The appropriateness of these 'exemptions' is discussed in Chapter 3.

39 *Privacy Act 1988*, s 18BB(2)(c).

40 Australian Government, *First stage response to ALRC Privacy Report*, 2009, recommendation 48-1, p. 89, www.dpmc.gov.au/privacy/reforms.cfm (accessed 13 September 2010).

41 Australian Government, *First stage response to ALRC Privacy Report*, 2009, recommendation 48-1, p. 89.

42 OPC, *Submission 16*, p. 12.

> Binding codes will allow greater flexibility in addressing privacy issues associated with new technologies or practices where industry has failed to effectively self-regulate and there is a compelling public interest in regulating these new practices or technologies…
>
> Such codes will allow the development of further detail on how the privacy principles apply in a particular circumstance. In this way, codes can provide specificity to the technology-neutral standards contained in the privacy principles.[43]

2.38 This approach was generally supported by consumer groups that appeared before the committee. Ms Teresa Corbin, CEO of ACCAN argued:

> Our general approach in relation to self-regulation [is], whilst we are happy for the industry to take initiatives and develop codes of practice that lift the bar and provide a model of best practice, we really do think that self-regulation has to be underpinned by a good regulatory framework in the first place, with the regulator having the ability to take strong enforcement action—not constantly, but when needed—and the power to do so when needed.[44]

2.39 However, organisations representing advertisers discussed the benefits of self-regulation and argued that it is currently working well. The Australian Association of National Advertisers (AANA) submitted that self-regulation is the best way to deal with privacy issues in online advertising, such as behavioural advertising, because of the speed at which technology changes.[45] The AANA submitted that self-regulation:

> …provides a flexible mechanism to meet the challenges of ever evolving advertising and marketing practices, media environment as well as consumer expectations.[46]

2.40 The AANA's CEO, Mr Scott McClellan argued that:

> A key benefit of this system is its ability to respond and adapt to evolving technology and changes in the way consumers access the media, both online and in the traditional sense. The AANA Code of Ethics, for example, is the overarching code for all Australian advertisers. It has the objective of ensuring that all advertising is ethical, and prepared with a proper sense of obligation to consumers and fairness to competitors.[47]

2.41 The AANA noted that it has had a self-regulatory framework since 1997 and has been proactive in addressing privacy issues. For example, the AANA submitted, that it has developed a code applying to marketing to children, which requires

---

43 OPC, *Submission 16*, p. 12.

44 Ms Teresa Corbin, CEO, ACCAN, *Committee Hansard*, 29 October 2010, p. 49.

45 AANA, *Submission 3*, p. 2.

46 AANA, *Submission 3*, p. 4.

47 Mr Scott McClellan, CEO, Australian Association of National Advertisers, *Committee Hansard*, 29 October 2010, p. 27.

advertisers to obtain parental consent before disclosing the personal information of any child.[48] Mr McClellan informed the committee that the AANA Code of Ethics is currently under review. A final report and revised Code of Ethics was expected to be submitted to the AANA Board in late 2010; however the AANA has decided to postpone finalising it pending the outcome of a current House of Representatives committee inquiry into the regulation of billboard and outdoor advertising.[49]

2.42 Similarly, the Communications Council expressed support for self-regulation as an effective way of protecting privacy online. The Council submitted that it has already developed online privacy guidelines, which it states 'serve to increase trust between advertisers and consumers, and to foster the protection of consumer's privacy'.[50] The Council submitted that it is also in the process of developing voluntary codes and standards on online behavioural advertising and the privacy of children online.[51]

2.43 According to Yahoo!7, there are ongoing discussions and attempts within the industry to develop standards and best-practice approaches.[52] Yahoo!7 argued that there are benefits to allowing the industry to self-regulate to a significant degree:

> Most advances in online privacy protection have come as a result of industry initiatives undertaken to preserve user trust in the Internet medium, and through self-regulatory efforts that allow competitor companies to recognise consistent best practices that reinforce consistent user experiences online…Market forces encourage companies like Yahoo!7 to bring privacy innovations to our customers quickly.[53]

2.44 Google agreed with these sentiments, arguing that service providers have a motivation to provide a safe and secure online environment to users in order to retain users' trust. Google submitted:

> This is most true in the highly competitive world of the web, where an alternative is just a click away.[54]

2.45 Mr Flynn, Head of Public Policy and Government Affairs, Google Australia, argued:

---

48 AANA, *Submission 3*, pp 2–3.

49 AANA media release, 'AANA leads discussion on advertising and marketing ethics', 5 August 2010; Mr Scott McClellan, CEO, AANA, *Committee Hansard*, 29 October 2010, p. 30; Ms A. Bain, Director of Codes, Policy and Regulatory Affairs, AANA, House of Representatives Standing Committee on Social Policy and Legal Affairs, *Proof Committee Hansard*, 24 February 2011, p. 2.

50 Communications Council, *Submission 12*, p. 3.

51 Communications Council, *Submission 12*, p. 4.

52 Yahoo!7, *Submission 2*, p. 3.

53 Yahoo!7, *Submission 2*, p. 5.

54 Google, *Submission 6*, p. 1.

> Our view is that service providers generally, and certainly Google, want their services associated with comfort, safety and security, and ultimately that is imperative to the providers' bottom line. Otherwise, if we do not get that right, internet users will switch, and on the internet that is very easy. A different service is literally just a click away. That choice, that ability to switch, is a key protection for individuals. They can easily move to another service or two if they so choose.[55]

2.46 Mrs Rohan, Director, Corporate and Regulatory Affairs, Australian Direct Marketing Association (ADMA), expressed similar views with respect to regulating the use of behavioural advertising (discussed in detail in chapter 3):

> Privacy is good business. That means that, if consumers do not trust you or they are concerned about privacy, they will not deal with you. They will not give you the information and they will move to competitors.[56]

2.47 Mr Leesong, CEO, Communications Council, agreed:

> It cannot be understated how important the preservation of the brand is. In fact, if an agency does deliver a poorly executed campaign which is in breach of privacy principles or is pulled up, it can be fatal to that agency's business.[57]

2.48 However, despite these arguments that online industries have self-interest in providing adequate privacy protection, Mr McClellan, CEO, AANA, noted that the development of codes and self-regulatory guidelines has not been as widespread as might have been expected when the Privacy Act was developed.[58]

2.49 In response to a question about what the 'shelf life' of an industry's attempts to self-regulate ought to be, Mr Leesong, CEO, Communications Council stated:

> It is a bit 'how long is a piece of string'. Self-regulation has been around for a long time. From a regulator's perspective, it is reasonable to expect to see the industry being proactive and keeping its codes up-to-date. It is reasonable to expect the industry to be communicating its activities to people like yourself, to interested parties. I would not want to put a time frame on it, but it would be more 'actions speak louder than words'. If there was a real absence of communications and activities, then I think, quite rightly, the industry would be leaving itself open to being regulated.[59]

---

55 Mr Iarla Flynn, Head of Public Policy and Government Affairs, Google Australia Pty Ltd, *Committee Hansard*, 29 October 2010, p. 2.

56 Mrs Melina Rohan, Director, Corporate and Regulatory Affairs, Australian Direct Marketing Association, *Committee Hansard*, 29 October 2010, p. 53.

57 Mr Daniel Leesong, CEO, Communications Council, *Committee Hansard*, 29 October 2010, p. 40.

58 Mr Scott McClellan, CEO, ADMA, *Committee Hansard*, 29 October 2010, p. 28.

59 Mr Daniel Leesong, CEO, Communications Council, *Committee Hansard*, 29 October 2010, p. 40.

2.50 Mr McClellan seemed to agree that despite a preference for self-regulation, there may be scope for further regulation by OPC where self-regulation is insufficient:

> I think it would be an interesting thing to look at whether—in the context of reviewing privacy legislation and its provision for sectoral codes, as Timothy Pilgrim [the Privacy Commissioner] alluded to just a moment ago—there may be scope for more work in this area, to address the nuances of particular industry sectors and how they go to market.[60]

2.51 Mr McClellan also noted that the Privacy Act plays an important role in underpinning industry codes.[61]

Committee comment

2.52 The committee accepts that there can be significant benefits to self-regulation. The committee also accepts that there are strong incentives for some companies and industries, such as the online advertising industry, to develop strong privacy protection practices in order that customers feel secure in dealing with those organisations. However, the committee is not convinced that this is always the case. The discussion in chapter 3 of this report regarding behavioural advertising demonstrates that it is frequently very lucrative for organisations to sell personal information, which increases the self-interest in having lax privacy protections, or loopholes in privacy policy. Accordingly, the committee supports in-principle the government's proposal to strengthen the powers of the OPC to develop and enforce industry codes for specific industries which pose risks to the privacy of Australians.

Education

2.53 The OPC submitted that 'user-education will be critical to ensuring that individuals are equipped to protect their privacy online', because of the fact that 'many aspects of online privacy remain in the hands of the individual'.[62]

2.54 The Victorian Privacy Commissioner agreed:

> Ensuring that individuals are fully informed and able to understand both the benefits and risks inherent in online interaction and engagement will be, by far, the most effective and efficient method, whether they are engaging in social networking services or transacting online.[63]

2.55 The key way in which individuals are informed about the privacy implications of providing personal information online is through website privacy policies. The Privacy Act requires private sector organisations covered by the Act to publish privacy policies setting out the purposes for which personal information is being collected and the uses to which it may be put.[64] This theoretically allows users to

---

60 Mr Scott McClellan, CEO, AANA, *Committee Hansard*, 29 October 2010, p. 28.

61 Mr Scott McClellan, CEO, AANA, *Committee Hansard*, 29 October 2010, p. 28.

62 OPC, *Submission 16*, p. 17.

63 Victorian Privacy Commissioner, *Submission 13*, p. 9.

64 Mr Timothy Pilgrim, Australian Privacy Commissioner, *Committee Hansard*, 29 October 2010, p. 22.

control their personal information by deciding whether or not to interact with an online organisation based on its stated privacy policies.

2.56 However, the Privacy Commissioner told the committee that:

> We hear constantly that privacy policies get extraordinarily complex and can become virtually worthless if people are not prepared to read them.[65]

2.57 The same point was made by a number of other witnesses that appeared before the committee.[66]

2.58 The committee heard about some best practice approaches, for example Google's use of videos to explain privacy features,[67] however to a large extent the complexity of a privacy policy and the quality of information available is dependent on the website operator.

2.59 Whilst acknowledging that at the end of the day, individual Internet users must inform themselves of what is going to happen to their information once they are online, the Privacy Commissioner advised the committee of the importance of finding new online privacy education approaches:

> So we have to find new mechanisms to allow people to understand what is going to happen to their personal information and be able to make educated choices before they enter into various transactions, or even when they are just browsing on the web—how do we educate the community? That is going to be one of the key areas.[68]

2.60 The OPC is empowered by the Privacy Act to undertake education programs in order to promote the protection of individual privacy.[69] In its review of Australian privacy law, the ALRC recommended that the OPC 'should develop and publish guidance in relation to technologies that impact on privacy',[70] which the government has indicated it supports.[71]

---

65 Mr Timothy Pilgrim, Australian Privacy Commissioner, *Committee Hansard*, 29 October 2010, p. 22.

66 Ms Teresa Corbin, CEO, ACCAN, *Committee Hansard*, 29 October 2010, p. 46; Ms Georgia King-Siem, Vice-President, Victorian Council for Civil Liberties (Liberty Victoria), *Committee Hansard*, 1 December 2010, p. 16; Ms Kathryn Miller, Member, Executive Committee; Member, Administrative Review and Constitutional Law Committee, Administrative Law and Human Rights Section, Law Institute of Victoria (LIV), *Committee Hansard*, 1 December 2010, p. 31.

67 Mr Iarla Flynn, Head of Public Policy and Government Affairs, Google Australia Pty Ltd, *Committee Hansard*, 29 October 2010, p. 11.

68 Mr Timothy Pilgrim, Australian Privacy Commissioner, *Committee Hansard*, 29 October 2010, p. 22.

69 *Privacy Act 1988*, para. 27(1)(m).

70 ALRC, *For Your Information: Australian Privacy Law and Practice*, Report No 108, 2008, recommendation 10-3.

71 Australian Government, *First stage response to ALRC Privacy Report*, 2009, p. 31.

2.61 The OPC has already developed educational materials on various issues concerning cyber safety including on:

- privacy issues faced by young people;
- social networking and spam; and
- smartphones.

2.62 The ACMA has also developed a number of education programs relating to online privacy issues:

> Under the brand name of Cybersmart...the ACMA distributes a diverse suite of cybersafety and cybersecurity programs. These target young people and those who are best able to influence young people's online engagement such as parents, teachers, trainee teachers and librarians. Our goal is to ensure that Australians have the skills, tools and knowledge to engage in the digital economy fully with trust and confidence. We recognise that building messages about privacy and the protection of personal privacy into education programs is central to achieving this goal.[72]

2.63 The ACMA informed the committee of some of its recent privacy education campaigns which include:

- the 'Z-card': 'a credit card sized fold-out pamphlet containing tips on how consumers can increase the security and privacy of their mobile phones'; and
- 'for Valentine's Day this year we targeted users of online dating sites with a postcard promotion designed to help them protect their identity and personal information when interacting with others online'.[73]

2.64 However, some submitters argued that more could still be done. For example, Mr Arved von Brasch submitted that education about online privacy should be included in the school curriculum.[74]

2.65 Ms Nerida O'Loughlin, General Manager, ACMA, informed the committee that while it is not mandatory for students to be educated about online privacy:

> ...our experience is that there is a very strong focus in most schools these days on embedding cybersafety and cybersecurity issues as much as they can in their work programs. The materials that we offer also complement other materials offered such as the ThinkUKnow program...[75]

2.66 Dr Roger Clarke, Chair of the Australian Privacy Foundation (APF), argued:

---

72 Ms Nerida O'Loughlin, General Manager, Digital Economy Division, Australian Communications and Media Authority, *Committee Hansard*, 1 December 2010, p. 56.

73 Ms Nerida O'Loughlin, General Manager, Digital Economy Division, Australian Communications and Media Authority, *Committee Hansard*, 1 December 2010, p. 56.

74 Mr Arved von Brasch, *Submission 2*, p. 2.

75 Ms Nerida O'Loughlin, General Manager, Digital Economy Division, Australian Communications and Media Authority, *Committee Hansard*, 1 December 2010, p. 57.

> Most real education that occurs is by peers...so it is about the kinds of features that are available and the way in which those features are used by the people seen by peers as being the smart ones—the leaders within the peer group. That is where the leadership needs to come from. That is why I stress this need for appropriate features in products, because if you make those features available then 'the street finds its uses for things'...[76]

2.67 In addition to educating the public about the privacy risks of providing personal information online, it is also important to educate those collecting and processing personal data. For example, the Community and Public Sector Union (CPSU) added that it is also important that public servants who received personal information that Australians have submitted online also need to be educated as to their obligations in both information sharing and privacy.[77]

2.68 Similarly, Mrs Melina Rohan, Director of Corporate and Regulatory Affairs, ADMA, discussed the importance of training advertisers about their privacy obligations, which is a service that ADMA provides:

> We provide compliance tools and websites. I teach a one-day compliance course 10 times a year. We have on call a 1-hour webinar which our marketers can access at any time. It highlights all of the requirements under the Privacy Act, the Do Not Call Register Act, the Spam Act, the Copyright Act and the Trade Practices Act.[78]

Privacy enhancing technology

2.69 The OPC submitted that technology may be configured to protect the privacy of individuals and limit the amount of information collected, for example by allowing individuals to remain anonymous, allowing websites to manage and obtain consent, or providing individuals with greater choice in relation to the secondary uses of their personal information.[79]

2.70 The committee received evidence from both Google and Yahoo!7 about their respective efforts to give users control over their privacy.

2.71 Google submitted that it takes privacy protection very seriously and has implemented a number of features which allow users to protect their privacy, including:

- *Google Dashboard* which allows users to control the privacy settings of their account;
- the ability for users to use 'incognito' mode in the *Chrome* browser, and to pause or delete their web history; and

---

76 Dr Roger Clarke, Chair, Australian Privacy Foundation, *Committee Hansard*, 1 December 2010, p. 12.

77 CPSU, *Submission 7*, p. 8.

78 Mrs Melina Rohan, Director, Corporate and Regulatory Affairs, ADMA, *Committee Hansard*, 29 October 2010, p. 58.

79 OPC, *Submission 16*, p. 18.

- encrypting *Gmail* by default.[80]

2.72 Yahoo!7 similarly submitted that it has voluntarily configured its sites to include privacy protections, including through:

> …easy navigation, information on special topics and [giving] prominence to our opt-out page, making it simple for users to find and exercise their privacy choices. We are also providing leadership in experimentation around ways to provide notice and transparency outside of standard privacy policies, thereby giving users multiple privacy touch points and greater insight into the ubiquity of data collection and its use online, notably around advertising.[81]

2.73 However, other witnesses argued that more could be done by companies like Google and Yahoo!7 to assist users in protecting their privacy. For example, Dr Clark, Chair, Australian Privacy Foundation (APF), argued that more facilities ought to be available to users who do not wish to log in and provide personal details.[82] Dr Clarke suggested that more would be achieved by meaningful and consultative discussion between major internet companies and public interest organisations, like APF.[83]

2.74 The OPC argued in its submission that:

> [W]hen privacy is 'designed into' new systems at a formative stage, those systems are more likely to protect and manage personal information effectively.[84]

2.75 The OPC suggested promoting these technologies in order to encourage their use and expand their availability and notes that the Canadian Office of the Privacy Commissioner allocates funding for non-profit research in the area.[85]

International Cooperation

2.76 One of the key difficulties with regulating online privacy results from the ease with which information can flow between jurisdictions. The OPC submitted that:

> Like other regulatory schemes, domestic privacy laws may struggle to cope with the ubiquitous nature of the internet.[86]

2.77 A number of international organisations have done work on this issue, developing various frameworks and making recommendations to member states.

2.78 For example, the Asia Pacific Economic Cooperation (APEC) adopted a Privacy Framework in 2004 which aims to encourage member states to develop

---

80 Google, *Submission 6*, p. 4.

81 Yahoo!7, *Submission 2*, p. 2.

82 Dr Roger Clarke, Chair, APF, *Committee Hansard*, 1 December 2010, p. 9.

83 Dr Roger Clarke, Chair, APF, *Committee Hansard*, 1 December 2010, pp 10–11.

84 OPC, *Submission 16*, p. 18.

85 OPC, *Submission 16*, p. 19.

86 OPC, *Submission 16*, p. 19.

appropriate privacy protections.[87] The strength of the APEC framework was criticised by a number of organisations during the course of this inquiry, aspects of which are discussed further in chapter 3.[88]

2.79 The Data Privacy Subgroup of APEC has recently developed a 'multi-lateral cross-border privacy enforcement arrangement for privacy enforcement authorities'.[89] The arrangement allows participating authorities to assist each other in collecting evidence, sharing information on investigations, enforcing actions and transferring complaints across jurisdictions. Australia's OPC is a co-administrator of the arrangement and was closely involved with its development.[90]

2.80 The Organisation for Economic Cooperation and Development (OECD) also has a number of projects aimed at developing international privacy protection standards, with which Australia is involved. The OECD developed privacy guidelines in 1980 which provided the model for Australia's privacy laws.[91] Like APEC, the OECD also has a network through which privacy enforcement authorities cooperate—called the Global Privacy Enforcement Network.[92]

Appropriateness of Australia's multi-faceted approach

2.81 As noted above, the OPC submitted that Australia needs to take a multi-faceted approach to privacy protection, utilising a range of formal and informal mechanisms to protect the privacy of Australians online.[93] A number of submitters, including the Victorian Privacy Commissioner, AANA and Google expressed support for this approach.[94] Mr Flynn, Head of Public Policy and Government Affairs, Google Australia, commented:

> Our view is that the best policy approach to privacy combines education with carefully framed laws and with technology tools that put internet users in the driving seat.[95]

2.82 The committee broadly accepts these arguments. Legislation and enforcement mechanisms are clearly necessary to underpin any privacy regime. Yet, given

---

87 Available at www.apec.org/apec/news___media/2004_media_releases/201104_apecminsendorseprivacyfrmwk.html (accessed 22 October 2010).

88 See Cyberspace Law and Policy Centre, *Submission 26*; APF, *Supplementary Submission 14*, p. 10.

89 OPC, *Submission 16*, p. 20.

90 OPC, *Submission 16*, p. 20.

91 OPC, *Submission 16*, p. 20.

92 OPC, *Submission 16*, p. 20.

93 OPC, *Submission 16*, p. 10.

94 OPC, *Submission 16*; Victorian Privacy Commissioner, *Submission 13*; Australian Association of National Advertisers, *Submission 3*.

95 Mr Iarla Flynn, Head of Public Policy and Government Affairs, Google Australia Pty Ltd, *Committee Hansard*, 29 October 2010, p. 1.

jurisdictional boundaries and the transnational nature of the Internet, it would be impossible for legislation alone to adequately protect the privacy of Australians online, and accordingly it is clear that educational programs and international engagement must form part of any successful approach to privacy.

2.83 Furthermore, in many situations it will be more appropriate to allow the market to decide what aspects of privacy individuals are willing to forego in exchange for the convenience of, for example, not needing to re-enter personal details for every transaction. Self-regulation will have a key role in this regard in setting industry best-practice benchmarks.

2.84 However, as will be discussed in chapters 3 and 4, it is not clear that Australia's approach always strikes the right balance between the various facets of its privacy protection framework. There was some disagreement amongst submitters as to the appropriate balance between the various approaches. For example, Ms King-Siem, Vice President, Liberty Victoria, argued that the Privacy Act ought to be strengthened in various ways, and play a greater role underpinning Australia's privacy framework:

> We believe that privacy is a fundamental human right. It is recognised under article 17 of the [International Covenant on Civil and Political Rights]. We do not believe that it is adequately protected in Australia. There is what I would term a patchwork of legislative protections that we have. For instance, in our federal Privacy Act there is an exemption for small business. Small business is, going on the Victorian Privacy Commissioner's submission, approximately 95 per cent of business in Australia, which means that 95 per cent of business is not subject to privacy regulation. There are employee information exemptions. All this adds up to what we feel is a less than adequate privacy regime in Australia.[96]

2.85 Furthermore, in relation to a number of emerging issues, it seems Australia's current approach to privacy regulation is applying offline thinking to online situations. The committee cautions that, as online technology continues to develop and new privacy issues emerge, it will be necessary to continually evaluate Australia's privacy framework to ensure that regulators are not simply applying old policy values and frameworks, which may be well suited to the offline contexts, to a very different online situation.

2.86 As Mr McDonald, Board Member, Communications Council cautioned:

> [Applying offline thinking to online problems] is probably not just an industry problem but a nationwide problem. As consumers change their habits change. But we continually like to put things in boxes and the boxes do not always frame the question well and are not always able to answer the problem correctly. There is a need for more dynamic, out-of-the-box

96 Ms Georgia King-Siem, Vice President, Victorian Council for Civil Liberties (Liberty Victoria), *Committee Hansard*, 1 December 2010, p. 15.

thinking about some of these problems, and not just online but thinking about privacy. Clearly, it does not work when you apply it to Facebook.[97]

97 Mr Iain McDonald, Board Member, Communications Council, *Committee Hansard*, 29 October 2010, p. 41.