Australian Government

Australian Government Response

to the

Senate Environment and Communications Reference Committee Report:

The adequacy of protections for the privacy of Australians online

November 2012

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.

Government Response

Noted. The report raises a number of relevant issues, with comments on the issues set out below: -

Communications privacy complaints: *In search of the right path* – Recommendations

1) There must be a significant improvement in time taken to resolve complaints at the OPC. The have significant resources, skills and expertise in privacy protections, and they only receive a tiny fraction of complaints in the sector. The OPC should aim to resolve the majority of complaints within 30 days.

   The Office of the Australian Information Commissioner (OAIC) receives a very small proportion of complaints about telecommunications but those that they do receives are usually complex. They involve issues such as the listing of debts with credit reporting agencies. The nature of such complaints makes them difficult to resolve quickly. Given this complexity, the OAIC has a current benchmark for finalising investigations of 150 days on average.

2) There must be a significant improvement in the information provided to individuals about resolution times. Information should be consistent (across the website, annual reports and verbal advice). It should be frank – e.g. exact timing targets, or an exact average based on prior complaints. It is very poor practice to accept a complaint without warning the consumer that it may take 6 months to resolve, especially when other avenues for resolution are available.

   The information should be consistent and based on average times and the OAIC will look to improve the information it currently provides to complainants.

3) All three complaint bodies (i.e. Australian Communications and Media Authority [ACMA], the Telecommunications Industry Ombudsman [TIO] and the OAIC) should undertake research to assess the demographic profiles of their complaints, to gain better understanding of special needs such as language and disability access. This research will also identify whether some disadvantaged groups are not utilising the services of these complaints bodies, and this information could be used to design outreach and targeting programs.

   The TIO has advised that it has developed a disadvantaged and vulnerable communications strategy, which identifies some targeted activities to research the needs of, and raise awareness of the TIO among, vulnerable groups in the community. These include culturally and linguistically diverse (CALD)

consumers, consumers in rural and regional areas, people with disabilities, indigenous consumers and young people.

The OAIC and the ACMA will look at the resource implications of undertaking such research.

4) There should be better coordination amongst the three complaints bodies, with the aim of reducing the adverse consequences for consumers of the current disconnection. A formal Memorandum of Understanding should be developed between the three complaint bodies. This agreement should include fair and transparent criteria for the management of complaints and for referrals between the three organisations. A process for sharing the identity of business parties to a complaint should be developed in order to enhance the recognition of systemic issues across the sector.

This recommendation is consistent with recommendation *73-8* from the Australian Law Reform Commission's (ALRC) Report 108 – *For Your Information: Australian Privacy Law and Practices*, which calls for the development of memoranda of understanding between the complaint handling bodies and clarity around the roles and responsibilities of each complaint handling organisation.

The ACMA has advised that a memorandum of understanding (MoU) has already been established between the ACMA and the TIO.

The OAIC has advised that it will explore developing a Memorandum of Understanding involving the three relevant complaints bodies.

5) Consumers should be provided with consistent information about where they should complain. This should include information on jurisdiction issues, but also on timelines and expected outcomes where these differ between the three complaints paths. It should be widely accessible and available to consumers contemplating or initiating complaints.

This recommendation is consistent with recommendation *73-9* from the Australian Law Reform Commission's (ALRC) Report 108 – *For Your Information: Australian Privacy Law and Practices*, calling for the OAIC to publish its complaint handling policies, procedures and enforcement guidelines, including the roles and functions of the complaints handling bodies under their relevant legislation.

The Department of Broadband, Communications and the Digital Economy, (DBCDE) has reviewed the role of the TIO and has recommended that the TIO clarify its jurisdiction over emerging products and services and publish information to establish clear boundaries around the issues, including complaints, that are within or outside its jurisdiction (see http://www.dbcde.gov.au/consultation and submissions/TIO reforms).

The OAIC's website offers a 'complaint checker' tool that assists potential complainants to identify the appropriate jurisdiction and to understand the complaint process and possible outcomes. The OAIC will consider whether the information provided to complainants can be enhanced to provide additional information, consistent with this recommendation.

6) Industry should be provided with consistent information about compliance. There should be no circumstances where the industry is receiving a message from one complaints body that everything is fine, while another complaints body is issuing warnings or enforcement action for non-compliance. Again this should be widely accessible and available for relevant industry personnel.

This could be one of the matters to be included in a MoU between the three bodies – see recommendations 4 and 5 above.

7) All three complaint bodies must ensure that they offer (and use) the full range of regulatory tools and remedies. These include:-

1. Compensation for the individual;
2. An apology for the individual;
3. Prompt correction or removal of personal data;
4. A change to business practice at the individual company;
5. A change to broader industry practice for systemic issues;
6. Occasional naming of individual companies as a warning to inform other consumers, and a lesson for industry that reputation consequences may arise from poor complaint outcomes; and
7. Occasional enforcement action in order to promote compliance.

In practice this recommendation will necessitate a change of approach at the OPC, so that they utilise their naming and enforcement powers, and a change of approach at the ACMA so that they offer greater individual remedies (such as compensation and apologies).

ACMA's recent *Reconnecting the Customer* inquiry and the DBCDE's review of the TIO may lead to regulatory change to improve industry behaviour and the end-user experience when seeking redress.

Currently, the OAIC employs a range of regulatory tools in the conduct of complaint handling activities. The Commissioner is able to seek each of the remedial actions listed above. The OAIC regularly seeks remedies 1 to 6, including the naming of respondents in reports of 'own motion' investigations and in the OAIC's annual report. Under the *Privacy Act 1988* (the Act) "enforcement action" would necessitate commencing action in the Federal Court to enforce a determination made under section 52 of the Act. The Commissioner also has a power to seek an injunction through the Federal Court to stop a person from engaging in conduct that would constitute a contravention of the Act.

The ALRC recommended and the Government agreed that the OAIC be granted with additional and improved powers to protect consumers in relation to privacy. The Privacy Amendment (Enhancing Privacy Protection) Bill 2012

includes amendments to strengthen the Information Commissioner's powers to conduct investigations, resolve complaints and promote compliance. These amendments will contribute to more effective and stronger protection of the right to privacy.

Recommendation 2

3.30 The committee recommends that the Australian Privacy Commissioner's complaint-handling role under paragraph 27(1) (ab) of the Privacy Act be expanded to more effectively address complaints about the misuse of privacy consent forms in the online context.

3.31 The committee further recommends that the Office of the Privacy Commissioner examine the issue of consent in the online context and develop guidelines on the appropriate use of privacy consent forms for online services.

Government Response

3.30 **Noted.** The ALRC recommended and the Government agreed that the OAIC be granted additional and improved powers to protect consumers in relation to privacy. The Privacy Amendment (Enhancing Privacy Protection) Bill 2012 includes amendments to strengthen the Information Commissioner's powers to conduct investigations, resolve complaints and promote compliance. These amendments will contribute to more effective and stronger protection of the right to privacy.

3.31 **Agreed in principle.** Implementation is a matter for the OAIC, taking account of available resources and priorities.

Recommendation 3

3.50 The committee recommends that the small business exemptions should be amended to ensure that small businesses which hold substantial quantities of personal information, or which transfer personal information offshore are subject to the requirements of the *Privacy Act 1988.*

3.51 To achieve this end, the committee urges the Australian Privacy Commissioner to undertake a review of those categories of small business with significant personal data holdings, and to make recommendations to government about expanding the categories of small business operators prescribed in regulations as subject to the *Privacy Act 1988.*

3.52 The committee further recommends that the second tranche of reforms to the *Privacy Act 1988* amend the Act to provide that all Australian organisations which transfer personal information overseas, including small businesses, must ensure that the information will be protected in a manner at least equivalent to the protections provided under Australia's privacy framework.

Government Responses

3.50 **Noted.** The Australian Law Reform Commission Report (ALRC) 108, *For Your Information: Australian Privacy Law and Practice* recommended (R39-1) that the Act be amended to remove the small business exemption.

The Government will take the recommendation into account when it considering the ALRC's recommendation to remove the small business exemption.

3.51 **Noted.** The Government will consider this recommendation in conjunction with its deliberations on recommendation 3.50 above.

3.52 **Noted.** The Government will consider this recommendation in conjunction with its deliberations on recommendations 3.50 and 3.51 above.

The Privacy Amendment (Enhancing Privacy Protection) Bill 2012 creates the Australian Privacy Principles, a single set of privacy principles applying to both Commonwealth agencies and private sector organisations. Australian Privacy Principle (APP) 8 and new section 16C will provide a framework for the regulation of cross-border disclosures of personal information. Before a cross-border disclosure can occur, the draft APP 8 imposes minimum obligations on an organisation to take such steps as are reasonable in the circumstances (for example, by imposing contractual obligations) to ensure that the overseas recipient does not breach the draft APPs.

In addition, an organisation will remain accountable for the acts and practices of the overseas recipient, unless an exemption applies.

Recommendation 4

3.86 The Committee recommends that the OPC in consultation with web browser developers, ISPs and the advertising industry, should, in accordance with proposed amendments to the Privacy Act, develop and impose a code which includes a 'Do Not Track' model following consultation with stakeholders.

Government Response

Noted. As part of its stage one response to the ALRC recommendations, the Government announced that it supports the development of binding and mandatory codes. Schedule 3 of the Privacy Amendment (Enhancing Privacy Protection) Bill 2012 contains the new provisions on privacy codes. It will be a matter for the Commissioner to consider whether a code is necessary.

Recommendation 5

3.96 The committee recommends that item 19(3) (g)(ii) of the exposure draft of amendments to the *Privacy Act 1988* be amended to provide that an organisation has an Australian link if it collects information *from* Australia, thereby ensuring that information collected from Australia in the online context is protected by the *Privacy Act 1988*.

Government Response

Noted. The Privacy Amendment (Enhancing Privacy Protection) Bill 2012 inserts the term 'Australian link' and lists additional connections with Australia which would be a sufficient link, see items 2-8 of Schedule 4 of the Bill.

Recommendation 6

3.109 The committee recommends that the government amend the *Privacy Act 1988* to require all Australian organisations that transfer personal information offshore are fully accountable for protecting the privacy of that information.

3.110 The committee further recommends that the government consider the enforceability of these provisions and, if necessary, strengthen the powers of the Australian Privacy Commissioner to enforce offshore data transfer provisions.

Government Response

Noted. See response to recommendation 3.52.

Recommendation 7

3.116 The committee recommends that the Australian government continue to work internationally, and particularly within our region, to develop strong privacy protections for Australians in the online context.

Government Response

Accepted. The Australian Government has been and will be continuing to work with appropriate international bodies including in particular regional bodies to further privacy protections.

The Government actively participates in the work of the Organisation for Economic Cooperation and Development (OECD) and Asian Pacific Economic Council (APEC) on international privacy issues. Australia has played a leading role in the development of the APEC Cross-Border Enforcement Arrangement (CPEA), which allows participating privacy regulators to share information and provide assistance in relation to privacy matters that have a cross-border aspect. The APEC CPEA commenced in July 2010 and the privacy regulators of Australia, Canada, New Zealand, Hong Kong China, and the United States are currently participants.

The OAIC continues to foster strong ties with other privacy authorities in the region via the Asia Pacific Privacy Authorities group.

Recommendation 8

3.122 The committee recommends that the government accept the ALRC's recommendation to legislate a cause of action for serious invasion of privacy.

Government Response

Noted. In July 2011, following publication of the Committee's report, the Government announced that it will bring forward consideration of those Australian Law Reform Commission (ALRC) Report 108, *For Your Information: Australian Privacy Law and Practice*, recommendations which relate to a statutory cause of action for serious invasion of privacy (chapter 74 of the ALRC Report). In September 2011, the Minister for Privacy and Freedom of Information Policy, the

Hon Brendan O'Connor, MP, released an issues paper as part of a community consultation to inform the Government's consideration of whether a cause of action should be legislated and, if so, how the elements of such a cause of action should be structured. The paper considers the ALRC's recommendations, relevant recommendations made by the New South Wales and Victorian law reform commissions, the current policy context and the legal position in Australian and other jurisdictions.

The Government will consider submissions received as part of the consultation process before determining whether to legislate for a Commonwealth cause of action and, if so, how legislation for such a cause of action should be drafted.

The Government will take the Committee's Recommendation 8 into account in making this determination.

Recommendation 9

4.74 The committee recommends that before pursuing any mandatory data retention proposal, the government must:

- undertake an extensive analysis of the costs, benefits and risks of such a scheme;
- justify the collection and retention of personal data by demonstrating the necessity of that data to law enforcement activities;
- quantify and justify the expense to Internet Service Providers of data collection and storage by demonstrating the utility of the data retained to law enforcement;
- assure Australians that data retained under any such scheme will be subject to appropriate accountability and monitoring mechanisms, and will be stored securely; and
- consult with a range of stakeholders.

Government Response

Agreed in principle. .The Government is committed to an open, transparent and consultative approach and acknowledges the public's interest in these issues.

The Parliamentary Joint Committee on Intelligence and Security is considering a range of measures that will allow law enforcement and intelligence agencies to meet the challenges of rapidly changing technology and the global security environment – including data retention.

The Government has not made a decision about whether or not Australia should have a data retention regime and the Government will consider the Committee's views before making any decisions.

Any proposal must strike an appropriate balance between community expectations regarding individual privacy and the investigation and prosecution of unlawful behaviour, as well as the provision of competitive commercial telecommunications services.