it is not stepping outside the bounds of my expertise to say that there would be significant public outcry. What we have here is the electronic equivalent, and it really means that the government is proposing to treat online privacy in a way that is different to offline privacy simply because the technology makes it possible.  

4.54 Ms Miller argued that there is no justification for treating online and offline privacy differently:

I do not think that people make that distinction in their personal lives, their private lives, their professional lives. We do not think that it is appropriate that the parliament make a distinction in legislation between online privacy and offline privacy.  

4.55 Ms Miller surmised that when it comes to the possible benefits of technology, law enforcement agencies seem to ask 'Can we do it?' as opposed to 'Is it appropriate or reasonable to do it?', and use invasive investigative techniques because they can, rather than because it is appropriate. She argued:

The question should always be 'Is it appropriate and reasonable?' It should not be the case that just because we can we will.  

4.56 Mr Pilgrim, Privacy Commissioner, agreed that it is not appropriate to distinguish between online and offline privacy simply because it is possible:

I would say that my position is that I would favour a consistent approach to data protection. I have not seen demonstrated necessarily why there should be any difference between whether the information is being handled online or offline. I have not seen a strong case put forward to explain that to me.  

4.57 In response to arguments by the Attorney-General's Department and the AFP that the proposal simply retains the status quo, requiring the retention of the same information that is available in relation to fixed-line telephone calls to be retained for

57 Ms Kathryn Miller, Member, Executive Committee; Member, Administrative Review and Constitutional Law Committee, Administrative Law and Human Rights Section, LIV, Committee Hansard, 1 December 2010, p. 24.

58 Ms Kathryn Miller, Member, Executive Committee; Member, Administrative Review and Constitutional Law Committee, Administrative Law and Human Rights Section, LIV, Committee Hansard, 1 December 2010, p. 25.

59 Ms Kathryn Miller, Member, Executive Committee; Member, Administrative Review and Constitutional Law Committee, Administrative Law and Human Rights Section, LIV, Committee Hansard, 1 December 2010, p. 25.

60 Ms Kathryn Miller, Member, Executive Committee; Member, Administrative Review and Constitutional Law Committee, Administrative Law and Human Rights Section, LIV, Committee Hansard, 1 December 2010, p. 25.

61 Mr Timothy Pilgrim, Australian Privacy Commissioner, Committee Hansard, 29 October 2010, p. 18.
online communications, many witnesses strongly disagreed. For example, Ms Miller argued:

The first distinction that I would make between call charge records and metadata of internet websites is that a phone number is just a phone number unless you have other information to interpret what the phone number is. And even if you know who owns the phone number and who the usual users of that number might be, you still know very little about the content of the conversation. I would suggest that when it comes to websites the website address and the type of information that is commonly found on that website can in fact be readily ascertained, even just from the metadata. So, even if the proposal is restricted to metadata as opposed to the actual web pages, there is still a great deal of extra information that can be obtained that you could not get from something like a call charge record.63

4.58 Another difference that Ms Miller noted was the important fact that data relating to fixed line telephone calls is collected for billing purposes, not law enforcement purposes. ISPs do not need to retain metadata for billing purposes, so that 'the only reason that they would be collecting this information is because it might be useful to law enforcement agencies not because of how they provide or charge for their service'.64

4.59 The LIV argued that this is inconsistent with key recommendations in the ALRC's report on Australian privacy law and practice, submitting that:

The large-scale collection of personal information by governments because it may be helpful to some government functions, rather than because it is necessary, constitutes a serious threat to online privacy. The power of the internet should not be used by governments to achieve measures of control that would not be possible without the internet.65

4.60 Ms King-Siem, Vice President, Liberty Victoria agreed:

I understand security issues, but this is where you take a targeted approach where there is a justification and reasonable suspicion that that information is required, not collect information and worry about it later. I think there is a tendency both at government and at corporate level—and in fact it is

63 Ms Kathryn Miller, Member, Executive Committee; Member, Administrative Review and Constitutional Law Committee, Administrative Law and Human Rights Section, LIV, Committee Hansard, 1 December 2010, p. 26.
64 Ms Kathryn Miller, Member, Executive Committee; Member, Administrative Review and Constitutional Law Committee, Administrative Law and Human Rights Section, LIV, Committee Hansard, 1 December 2010, p. 26.
66 LIV, Submission 9, p. 2. Emphasis in original.
perhaps just a natural tendency—to collect more than you need and then swallow it later.67

Will the data be useful for law enforcement

4.61 Finally, a number of witnesses and submitters questioned whether the data proposed to be retained would even be of use to law enforcement.

4.62 The LIV argued that the proposed regime would be 'unworkable for law enforcement agencies' due to the huge amounts of data collected.68

4.63 Ms Miller, LIV, also argued that the proposal is unnecessary as:

Law enforcement agencies can currently apply for warrants to obtain information such as browsing histories from ISPs. If there is a concern that some ISPs do not contain significant browsing history, then the LIV considers that that can be dealt with on a case-by-case basis.69

4.64 There is also a risk that a data retention scheme will be ineffective because criminals and others wishing to evade detection will simply use the various mechanisms available to them to hide their online identity. The committee received evidence of various international online services dedicated to protecting the identity of domain name owners. For example, Fraudwatch International submitted that:

Some domain registrars now provide a "Domain Privacy Protection" service, where the domain owners contact information is not listed in the WHOIS database, but is replaced by standard contact information for either the domain registrar or the privacy service, making it virtually impossible to actually find, or contact the real owner of the domain.70

4.65 This obviously makes it incredibly difficult to identify the owners of fraudulent phishing websites and shut them down. Mr Trent Youl, CEO, Fraudwatch International, informed the committee that:

One of the issues we face when we are trying to have phishing websites taken down is that we find a hacked website and suddenly we cannot contact the website owner because their information is hidden. If the website owner has subscribed to this type of service that is apparently protecting their privacy and they do not have any contact information on their website, which many websites do not, it makes it very difficult for us sometimes to do our job and get these fraudulent websites taken down as quickly as possible.71

---

67 Ms Georgia King-Slem, Vice-President, Liberty Victoria, Committee Hansard, 1 December 2010, p. 16.
68 LIV, Submission 9, p. 2.
69 Ms Kathryn Miller, Member, Executive Committee; Member, Administrative Review and Constitutional Law Committee, Administrative Law and Human Rights Section, LIV, Committee Hansard, 1 December 2010, p. 24.
70 Fraudwatch International, Submission 22, p. 2.
71 Mr Trent Youl, CEO, Fraudwatch International Pty Ltd, Committee Hansard, 29 October 2010, p. 74.
4.66 Fraudwatch submitted that domain privacy protection:

...allows people to anonymously run websites which may be using dubious business practices, fraud, or theft [and] it allows criminals to hide their contact information and appear to be legitimate.\(^2\)

4.67 There is a good chance that increased law enforcement monitoring of online communications will result in the proliferation of this, and similar options for internet users to hide their identity, provided that they are sufficiently tech-savvy. Mr Jacobs, Chair, EFA, explained:

Given that you can host a website in any country and given that regulations vary, the way the internet works is anonymity is something that is probably going to apply to people who run websites as well as people who use them. So I think it is inevitable that such technology will exist. We will see a bit of an arms race when it comes to the technology itself and, perhaps, with the laws; but, no, I do not find that surprising. I think it is inevitable. We will have to have other ways to deal with it.\(^3\)

4.68 There are already services available for consumers who wish to evade the EU’s data retention scheme and other monitoring, such as Tor\(^4\) and the Invisible Internet Project (I2P).\(^5\)

**Committee comment**

4.69 The committee has a number of concerns, both with the Attorney-General’s Department’s data retention proposal itself, as well as with the way the consultation process has been handled so far.

4.70 There is a lot of misinformation and rumour about the scheme, and it seems to the committee that this is largely due to the Attorney-General’s Department’s narrow consultations on the issue to date. While industry has been consulted, there has not yet been any discussion with the broader community or public interest and civil liberties organisations. While the committee acknowledges the Attorney-General’s Department’s explanation for this,\(^6\) the lack of information available to the public about the proposal has resulted in confusion, mistrust and fear about the proposal.

4.71 The committee’s central concerns about the proposal are the very real possibilities that it is unnecessary, will not provide sufficient benefit to law enforcement agencies, and is disproportionate to the end sought to be achieved. The proposal has very serious privacy implications, even if one accepts the arguments of the Attorney-General’s Department and AFP that the same information is already available for fixed-line telephone records. The fact is that much of the information

---

72 Fraudwatch International, Submission 22, p. 4.
73 Mr Colin Jacobs, Chair, EFA, Committee Hansard, 29 October 2010, p. 67.
76 Ms Catherine Smith, Assistant Secretary, Telecommunications and Surveillance Law Branch, Attorney-General’s Department, Committee Hansard, 1 December 2010, p. 48.
intended to form part of the scheme does not need to be collected for any other purpose, so the only reason to retain it is the mere possibility that it may prove useful to law enforcement. This seems to the committee to be a significant departure from the core principles underpinning Australia's privacy regulation.

4.72 Furthermore, the committee considers that there is a very real risk that the most serious, tech-savvy criminals—particularly those involved in fraud and child pornography—will be able to evade monitoring in any respect as a result of technological developments.

4.73 Accordingly, the committee urges that prior to any proposal for data retention going any further, an extensive analysis of the costs, benefits and risks of such a scheme must be undertaken. Before pursuing such a scheme, it is incumbent upon government to:

- prove that the information is necessary to law enforcement agencies and justifies such a significant intrusion on the privacy of all Australians;
- quantify and justify the expense to ISPs and other companies which will be required to retain data under such a scheme;
- implement strong and appropriate accountability and monitoring mechanisms, and ensure that data retained under the scheme is able to be, and will in fact be, stored securely; and
- consult with a wide range of stakeholders on the proposal, including, but not limited to, civil liberties and public interest advocates, privacy policy experts such as the Australian Privacy Foundation, in particular.

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.
4.75 The committee notes that the government is reviewing cyber security and cyber crime as part of its response to the recommendations of the recent House of Representatives committee report into Cyber crime (see paragraph 1.7). The committee encourages the government to take the recommendations contained in this report into account in that review. The committee also expects the government will respond separately to the recommendations made in this report in the usual manner, noting that the Senate has declared that responses should be tabled within 3 months. 

Senator Mary Jo Fisher
Chair

Senator Doug Cameron
Deputy Chair

Senator Scott Ludlam


Appendix 1

Submissions, tabled documents and answers to questions taken on notice

<table>
<thead>
<tr>
<th>No.</th>
<th>Submission</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Mr Arved von Brasch</td>
</tr>
<tr>
<td>2</td>
<td>Yahoo!7 Pty Ltd</td>
</tr>
<tr>
<td>3</td>
<td>Australian Association of National Advertisers</td>
</tr>
<tr>
<td>4</td>
<td>Mr Rodney Serkowski, Pirate Party Australia</td>
</tr>
<tr>
<td>5</td>
<td>Confidential</td>
</tr>
<tr>
<td>6</td>
<td>Google Australia Pty Ltd</td>
</tr>
<tr>
<td>7</td>
<td>Community and Public Sector Union (CPSU)</td>
</tr>
<tr>
<td>8</td>
<td>Mr Alastair MacGibbon, Internet Safety Institute</td>
</tr>
<tr>
<td>9</td>
<td>Law Institute of Victoria</td>
</tr>
<tr>
<td>10</td>
<td>Australian Council of Trade Unions</td>
</tr>
<tr>
<td>11</td>
<td>Australian Communications Consumer Action Network (ACCAN)</td>
</tr>
<tr>
<td>12</td>
<td>The Communications Council</td>
</tr>
<tr>
<td>13</td>
<td>Office of the Victorian Privacy Commissioner</td>
</tr>
<tr>
<td>14</td>
<td>Australian Privacy Foundation</td>
</tr>
<tr>
<td>15</td>
<td>Australian Direct Marketing Association</td>
</tr>
<tr>
<td>16</td>
<td>Office of the Privacy Commissioner</td>
</tr>
<tr>
<td>17</td>
<td>Rule of Law Institute of Australia</td>
</tr>
<tr>
<td>18</td>
<td>Name Withheld</td>
</tr>
<tr>
<td>19</td>
<td>Name Withheld</td>
</tr>
<tr>
<td>20</td>
<td>Electronic Frontiers Australia</td>
</tr>
<tr>
<td>21</td>
<td>Mr John Scott</td>
</tr>
<tr>
<td>22</td>
<td>FraudWatch International Pty Ltd</td>
</tr>
<tr>
<td>23</td>
<td>Australian Federation of AIDS Organisations (AFAO)</td>
</tr>
<tr>
<td>24</td>
<td>Dr George Barker</td>
</tr>
<tr>
<td>25</td>
<td>Business Council of Australia</td>
</tr>
<tr>
<td>26</td>
<td>Mr Nigel Waters, Cyberspace Law + Policy Centre, Faculty of Law, UNSW</td>
</tr>
<tr>
<td>27</td>
<td>Australian Youth Affairs Coalition</td>
</tr>
<tr>
<td>28</td>
<td>Macquarie Telecom</td>
</tr>
</tbody>
</table>

RELEASED UNDER THE FOI ACT 1982 BY
THE ATTORNEY-GENERAL'S DEPARTMENT
Tabled documents

Distribution list for March 2010 data retention consultation meeting – Communications Alliance (tabled by the Attorney-General's Department, public hearing, Canberra, 29 October 2010).

Opening statement by Ms Catherine Smith, Assistant Secretary, Telecommunications and Surveillance Law Branch, Attorney-General's Department (public hearing, Canberra, 29 October 2010).

Answers to questions taken on notice

1. Attorney-General's Department - Answers to questions taken on notice (from public hearing 29 October 2010)

2. Australian Association of National Advertisers - Answers to questions taken on notice (from public hearing 29 October 2010)

3. The Communications Council - Answers to questions taken on notice (from public hearing 29 October 2010)

4. Liberty Victoria - Answers to questions taken on notice (from public hearing 1 December 2010)

5. Liberty Victoria - Answers to questions taken on notice (from public hearing 1 December 2010)

6. Australian Council of Trade Unions - Answers to questions taken on notice (from public hearing 1 December 2010)

7. Google - Answers to questions taken on notice (from public hearing 29 October 2010)

8. Australian Direct Marketing Association - Answers to questions taken on notice (from public hearing 29 October 2010)

9. Law Institute Victoria - Answers to questions taken on notice (from public hearing 1 December 2010)
Appendix 2

Public hearings

*Friday, 29 October 2010 – Canberra*

**Google Australia Pty Ltd**

- Mr Iarla Flynn, Head, Public Policy and Government Affairs
- Ms Ishtar Vij, Manager, Public and Policy and Government Affairs

**Office of the Privacy Commissioner**

- Mr Timothy Pilgrim, Australian Privacy Commissioner
- Ms Angelene Falk, Director, Policy

**Australian Association of National Advertisers**

- Mr Scott McClellan, Chief Executive Officer

**The Communications Council**

- Mr Daniel Leesong, Chief Executive Officer
- Mr Iain McDonald, Board Member
- Ms Linde Wolters, Media and Public Affairs

**Australian Communications Consumer Action Network**

- Ms Teresa Corbin, Chief Executive Officer

**Australian Direct Marketing Association**

- Mrs Melina Rohan, Director, Corporate and Regulatory Affairs

**Electronic Frontiers Australia**

- Mr Colin Jacobs, Chair

**Fraudwatch International Pty Ltd**

- Mr Trent B Youl, Chief Executive Officer
Department of Broadband, Communications and the Digital Economy

Mr Keith Besgrove, First Assistant Secretary, Digital Economy Services
Ms Wendy Kelly, Director, Telecommunications and Surveillance Law Branch
Mr Duncan McIntyre, Assistant Secretary, Consumer Policy and Post
Ms Joan Sheedy, Assistant Secretary, Privacy and Freedom of Information Policy Branch
Ms Catherine Smith, Assistant Secretary, Telecommunications and Surveillance Law Branch

Australian Federal Police

Assistant Commissioner Neil Gaughan, National Manager, High Tech Crime Operations
Mr Peter Whowell, Manager, Government Relations

Wednesday, 1 December 2010 – Melbourne

Australian Privacy Foundation

Dr Roger Clarke, Chair

Victorian Council for Civil Liberties (Liberty Victoria)

Ms Georgie King-Siem, Vice-President

Law Institute of Victoria

Ms Kathryn Miller, Member, Executive Committee; Member, Administrative Review and Constitutional Law Committee, Administrative Law and Human Rights Section

Australian Council of Trade Unions

Mr Trevor Clarke, Legal and Industrial Officer
Mr Joel Fetter, Policy and Industrial Director

Australian Federal Police

Commander Alan Scott, Manager, Melbourne Office
Mr Peter Whowell, Manager, Government Relations
Attorney-General's Department

Ms Wendy Kelly, Director, Telecommunications and Surveillance Law Branch

Ms Catherine Smith, Assistant Secretary, Telecommunications and Surveillance Law Branch

Australian Communications and Media Authority

Ms Olya Booyar, General Manager, Content, Consumer and Citizen Division

Ms Nerida O'Loughlin, General Manager, Digital Economy Division

Ms Jonquil Ritter, Executive Manager, Citizen and Community Branch, Content, Consumer and Citizen Division

Ms Andree Wright, Executive Manager, Security Safety and e-Education Branch, Digital Economy Division
Appendix 3

Information Privacy Principles, National Privacy Principles, and proposed Australian Privacy Principles

Information Privacy Principles
(Privacy Act 1988, section 14)

Principle 1

Manner and purpose of collection of personal information

1. Personal information shall not be collected by a collector for inclusion in a record or in a generally available publication unless:
   (a) the information is collected for a purpose that is a lawful purpose directly related to a function or activity of the collector; and
   (b) the collection of the information is necessary for or directly related to that purpose.

2. Personal information shall not be collected by a collector by unlawful or unfair means.

Principle 2

Solicitation of personal information from individual concerned

Where:
   (a) a collector collects personal information for inclusion in a record or in a generally available publication; and
   (b) the information is solicited by the collector from the individual concerned;
the collector shall take such steps (if any) as are, in the circumstances, reasonable to ensure that, before the information is collected or, if that is not practicable, as soon as practicable after the information is collected, the individual concerned is generally aware of:
   (c) the purpose for which the information is being collected;
   (d) if the collection of the information is authorised or required by or under law—the fact that the collection of the information is so authorised or required; and
   (e) any person to whom, or any body or agency to which, it is the collector's usual practice to disclose personal information of the kind so collected, and (if known by the collector) any person to whom, or any body or agency to which, it is the usual practice of that first-mentioned person, body or agency to pass on that information.

Principle 3

Solicitation of personal information generally
Where:
(a) a collector collects personal information for inclusion in a record or in a generally available publication; and
(b) the information is solicited by the collector;
the collector shall take such steps (if any) as are, in the circumstances, reasonable to ensure that, having regard to the purpose for which the information is collected:
(c) the information collected is relevant to that purpose and is up to date and complete; and
(d) the collection of the information does not intrude to an unreasonable extent upon the personal affairs of the individual concerned.

Principle 4

Storage and security of personal information

A record-keeper who has possession or control of a record that contains personal information shall ensure:
(a) that the record is protected, by such security safeguards as it is reasonable in the circumstances to take, against loss, against unauthorised access, use, modification or disclosure, and against other misuse; and
(b) that if it is necessary for the record to be given to a person in connection with the provision of a service to the record-keeper, everything reasonably within the power of the record-keeper is done to prevent unauthorised use or disclosure of information contained in the record.

Principle 5

Information relating to records kept by record-keeper

1. A record-keeper who has possession or control of records that contain personal information shall, subject to clause 2 of this Principle, take such steps as are, in the circumstances, reasonable to enable any person to ascertain:
(a) whether the record-keeper has possession or control of any records that contain personal information; and
(b) if the record-keeper has possession or control of a record that contains such information:
   (i) the nature of that information;
   (ii) the main purposes for which that information is used; and
   (iii) the steps that the person should take if the person wishes to obtain access to the record.

2. A record-keeper is not required under clause 1 of this Principle to give a person information if the record-keeper is required or authorised to refuse to give that information to the person under the applicable provisions of any law of the Commonwealth that provides for access by persons to documents.

3. A record-keeper shall maintain a record setting out:
(a) the nature of the records of personal information kept by or on behalf of the record-keeper;
(b) the purpose for which each type of record is kept;
(c) the classes of individuals about whom records are kept;
(d) the period for which each type of record is kept;
(e) the persons who are entitled to have access to personal information contained in the
records and the conditions under which they are entitled to have that access; and
(f) the steps that should be taken by persons wishing to obtain access to that
information.

4. A record-keeper shall:
   (a) make the record maintained under clause 3 of this Principle available for inspection
       by members of the public; and
   (b) give the Commissioner, in the month of June in each year, a copy of the record so
       maintained.

**Principle 6**

**Access to records containing personal information**

Where a record-keeper has possession or control of a record that contains personal
information, the individual concerned shall be entitled to have access to that record,
except to the extent that the record-keeper is required or authorised to refuse to provide
the individual with access to that record under the applicable provisions of any law of the
Commonwealth that provides for access by persons to documents.

**Principle 7**

**Alteration of records containing personal information**

1. A record-keeper who has possession or control of a record that contains personal
   information shall take such steps (if any), by way of making appropriate corrections,
deletions and additions as are, in the circumstances, reasonable to ensure that the record:
   (a) is accurate; and
   (b) is, having regard to the purpose for which the information was collected or is to be
       used and to any purpose that is directly related to that purpose, relevant, up to date,
complete and not misleading.

2. The obligation imposed on a record-keeper by clause 1 is subject to any applicable
   limitation in a law of the Commonwealth that provides a right to require the correction or
   amendment of documents.

3. Where:
   (a) the record-keeper of a record containing personal information is not willing to
       amend that record, by making a correction, deletion or addition, in accordance with
       a request by the individual concerned; and
   (b) no decision or recommendation to the effect that the record should be amended
       wholly or partly in accordance with that request has been made under the
       applicable provisions of a law of the Commonwealth;

   the record-keeper shall, if so requested by the individual concerned, take such steps (if
   any) as are reasonable in the circumstances to attach to the record any statement provided
   by that individual of the correction, deletion or addition sought.
Principle 8

Record-keeper to check accuracy etc. of personal information before use

A record-keeper who has possession or control of a record that contains personal information shall not use that information without taking such steps (if any) as are, in the circumstances, reasonable to ensure that, having regard to the purpose for which the information is proposed to be used, the information is accurate, up to date and complete.

Principle 9

Personal information to be used only for relevant purposes

A record-keeper who has possession or control of a record that contains personal information shall not use the information except for a purpose to which the information is relevant.

Principle 10

Limits on use of personal information

1. A record-keeper who has possession or control of a record that contains personal information that was obtained for a particular purpose shall not use the information for any other purpose unless:
   (a) the individual concerned has consented to use of the information for that other purpose;
   (b) the record-keeper believes on reasonable grounds that use of the information for that other purpose is necessary to prevent or lessen a serious and imminent threat to the life or health of the individual concerned or another person;
   (c) use of the information for that other purpose is required or authorised by or under law;
   (d) use of the information for that other purpose is reasonably necessary for enforcement of the criminal law or of a law imposing a pecuniary penalty, or for the protection of the public revenue; or
   (e) the purpose for which the information is used is directly related to the purpose for which the information was obtained.

2. Where personal information is used for enforcement of the criminal law or of a law imposing a pecuniary penalty, or for the protection of the public revenue, the record-keeper shall include in the record containing that information a note of that use.

Principle 11

Limits on disclosure of personal information

1. A record-keeper who has possession or control of a record that contains personal information shall not disclose the information to a person, body or agency (other than the individual concerned) unless:
(a) the individual concerned is reasonably likely to have been aware, or made aware under Principle 2, that information of that kind is usually passed to that person, body or agency;
(b) the individual concerned has consented to the disclosure;
(c) the record-keeper believes on reasonable grounds that the disclosure is necessary to prevent or lessen a serious and imminent threat to the life or health of the individual concerned or of another person;
(d) the disclosure is required or authorised by or under law; or
(e) the disclosure is reasonably necessary for the enforcement of the criminal law or of a law imposing a pecuniary penalty, or for the protection of the public revenue.

2. Where personal information is disclosed for the purposes of enforcement of the criminal law or of a law imposing a pecuniary penalty, or for the purpose of the protection of the public revenue, the record-keeper shall include in the record containing that information a note of the disclosure.

3. A person, body or agency to whom personal information is disclosed under clause 1 of this Principle shall not use or disclose the information for a purpose other than the purpose for which the information was given to the person, body or agency.
National Privacy Principles
(Privacy Act 1988, Schedule 3)

1 Collection

1.1 An organisation must not collect personal information unless the information is necessary for one or more of its functions or activities.

1.2 An organisation must collect personal information only by lawful and fair means and not in an unreasonably intrusive way.

1.3 At or before the time (or, if that is not practicable, as soon as practicable after) an organisation collects personal information about an individual from the individual, the organisation must take reasonable steps to ensure that the individual is aware of:
   (a) the identity of the organisation and how to contact it; and
   (b) the fact that he or she is able to gain access to the information; and
   (c) the purposes for which the information is collected; and
   (d) the organisations (or the types of organisations) to which the organisation usually discloses information of that kind; and
   (e) any law that requires the particular information to be collected; and
   (f) the main consequences (if any) for the individual if all or part of the information is not provided.

1.4 If it is reasonable and practicable to do so, an organisation must collect personal information about an individual only from that individual.

1.5 If an organisation collects personal information about an individual from someone else, it must take reasonable steps to ensure that the individual is or has been made aware of the matters listed in subclause 1.3 except to the extent that making the individual aware of the matters would pose a serious threat to the life or health of any individual.

2 Use and disclosure

2.1 An organisation must not use or disclose personal information about an individual for a purpose (the secondary purpose) other than the primary purpose of collection unless:
   (a) both of the following apply:
      (i) the secondary purpose is related to the primary purpose of collection and, if the personal information is sensitive information, directly related to the primary purpose of collection;
      (ii) the individual would reasonably expect the organisation to use or disclose the information for the secondary purpose; or
   (b) the individual has consented to the use or disclosure; or
   (c) if the information is not sensitive information and the use of the information is for the secondary purpose of direct marketing:
      (i) it is impracticable for the organisation to seek the individual’s consent before that particular use; and
      (ii) the organisation will not charge the individual for giving effect to a request by the individual to the organisation not to receive direct marketing communications; and
      (iii) the individual has not made a request to the organisation not to receive direct marketing communications; and
(iv) in each direct marketing communication with the individual, the organisation
draws to the individual's attention, or prominently displays a notice, that he or
she may express a wish not to receive any further direct marketing
communications; and

(v) each written direct marketing communication by the organisation with the
individual (up to and including the communication that involves the use) sets
out the organisation's business address and telephone number and, if the
communication with the individual is made by fax, telex or other electronic
means, a number or address at which the organisation can be directly
contacted electronically; or

(d) if the information is health information and the use or disclosure is necessary for
research, or the compilation or analysis of statistics, relevant to public health or
public safety:

(i) it is impracticable for the organisation to seek the individual's consent before
the use or disclosure; and

(ii) the use or disclosure is conducted in accordance with guidelines approved by
the Commissioner under section 95A for the purposes of this subparagraph; and

(iii) in the case of disclosure—the organisation reasonably believes that the
recipient of the health information will not disclose the health information, or
personal information derived from the health information; or

(e) the organisation reasonably believes that the use or disclosure is necessary to lessen
or prevent:

(i) a serious and imminent threat to an individual's life, health or safety; or

(ii) a serious threat to public health or public safety; or

(ea) if the information is genetic information and the organisation has obtained the
genetic information in the course of providing a health service to the individual:

(i) the organisation reasonably believes that the use or disclosure is necessary to
lesser or prevent a serious threat to the life, health or safety (whether or not
the threat is imminent) of an individual who is a genetic relative of the
individual to whom the genetic information relates; and

(ii) the use or disclosure is conducted in accordance with guidelines approved by
the Commissioner under section 95AA for the purposes of this subparagraph; and

(iii) in the case of disclosure—the recipient of the genetic information is a genetic
relative of the individual; or

(f) the organisation has reason to suspect that unlawful activity has been, is being or
may be engaged in, and uses or discloses the personal information as a necessary
part of its investigation of the matter or in reporting its concerns to relevant persons
or authorities; or

(g) the use or disclosure is required or authorised by or under law; or

(h) the organisation reasonably believes that the use or disclosure is reasonably
necessary for one or more of the following by or on behalf of an enforcement body:

(i) the prevention, detection, investigation, prosecution or punishment of criminal
offences, breaches of a law imposing a penalty or sanction or breaches of a
prescribed law;

(ii) the enforcement of laws relating to the confiscation of the proceeds of crime;

(iii) the protection of the public revenue;

(iv) the prevention, detection, investigation or remedying of seriously improper
conduct or prescribed conduct;
(v) the preparation for, or conduct of, proceedings before any court or tribunal, or implementation of the orders of a court or tribunal.

Note 1: It is not intended to deter organisations from lawfully co-operating with agencies performing law enforcement functions in the performance of their functions.

Note 2: Subclause 2.1 does not override any existing legal obligations not to disclose personal information. Nothing in subclause 2.1 requires an organisation to disclose personal information; an organisation is always entitled not to disclose personal information in the absence of a legal obligation to disclose it.

Note 3: An organisation is also subject to the requirements of National Privacy Principle 9 if it transfers personal information to a person in a foreign country.

2.2 If an organisation uses or discloses personal information under paragraph 2.1(h), it must make a written note of the use or disclosure.

2.3 Subclause 2.1 operates in relation to personal information that an organisation that is a body corporate has collected from a related body corporate as if the organisation’s primary purpose of collection of the information were the primary purpose for which the related body corporate collected the information.

2.4 Despite subclause 2.1, an organisation that provides a health service to an individual may disclose health information about the individual to a person who is responsible for the individual if:
(a) the individual:
   (i) is physically or legally incapable of giving consent to the disclosure; or
   (ii) physically cannot communicate consent to the disclosure; and
(b) a natural person (the carer) providing the health service for the organisation is satisfied that either:
   (i) the disclosure is necessary to provide appropriate care or treatment of the individual; or
   (ii) the disclosure is made for compassionate reasons; and
(c) the disclosure is not contrary to any wish:
   (i) expressed by the individual before the individual became unable to give or communicate consent; and
   (ii) of which the carer is aware, or of which the carer could reasonably be expected to be aware; and
(d) the disclosure is limited to the extent reasonable and necessary for a purpose mentioned in paragraph (b).

2.5 For the purposes of subclause 2.4, a person is responsible for an individual if the person is:
(a) a parent of the individual; or
(b) a child or sibling of the individual and at least 18 years old; or
(c) a spouse or de facto partner of the individual; or
(d) a relative of the individual, at least 18 years old and a member of the individual’s household; or
(e) a guardian of the individual; or
(f) exercising an enduring power of attorney granted by the individual that is exercisable in relation to decisions about the individual’s health; or
(g) a person who has an intimate personal relationship with the individual; or
(h) a person nominated by the individual to be contacted in case of emergency.

2.6 In subclause 2.5: