



**Australian Government**

---

**Office of the Privacy Commissioner**

# **Digital Economy Future Directions: Consultation Paper**

**Submission to Department of  
Broadband, Communications  
and the Digital Economy**

**February 2009**

## Key recommendations

1. The Office of the Privacy Commissioner (the Office) welcomes the opportunity to provide input into the development of the *Digital Economy Future Directions Paper* (the Future Directions Paper) by the Department of Broadband, Communications and the Digital Economy (the Department).
2. It is the Office's view that privacy has an important and integral part to play in the digital economy. In particular the Office believes that embedding privacy protections in the design of networked information and communication technology (ICT) systems will garner trust amongst individuals and organisations. This will help to ensure that Australia fully realises the opportunities offered by the digital economy.
3. On this basis, the Office recommends that the Department consider:
  - encouraging a multi-faceted approach to enhancing privacy in the development of the digital economy to supplement the protections offered by the *Privacy Act 1988*. A multi-faceted approach could include: educating individuals about protecting their information when using digital technologies; harnessing privacy enhancing technologies; and participating in international agreements and initiatives between jurisdictions (see pars. 17-18).
  - including a section on privacy enhancing technologies which recognises their importance to furthering Australia's participation in the digital economy (see pars. 27-30).
  - providing examples of notable privacy enhancing technologies amongst the case studies. The Office would be happy to work with the Department on identifying appropriate privacy enhancing technology case studies (see par. 31).
  - emphasising the importance of privacy impact assessments to embedding privacy protections in new ICT systems (see pars. 32-39).
  - referencing the ongoing work of international forums such as APEC to enhance privacy protections around transborder data flows. Aimed at enhancing consumer confidence and thus supporting the expansion of electronic commerce, the work of these forums is important to Australia's domestic participation in the digital economy (see pars. 41-50).
  - exploring options to encourage privacy-friendly identity management processes by businesses transacting online (see pars. 54-59).
  - including examples or case studies of good identity management systems to highlight opportunities for enhancing participation in the digital economy. The Office would be happy to work with the Department to identify appropriate identity management systems for this purpose (see par. 60).
4. The Office also makes suggestions in relation to some of the specific questions raised in the consultation draft of the Future Directions Paper.

## Office of the Privacy Commissioner

5. The Office of the Privacy Commissioner (the Office) is an independent statutory body whose purpose is to promote and protect privacy in Australia. The Office, established under the *Privacy Act 1988* (Cth) (the Privacy Act), has responsibilities for the protection of individuals' personal information that is handled by Australian and ACT Government agencies, and personal information held by all large private sector organisations, health service providers and some small businesses.

## Overview

6. The Office welcomes the opportunity to provide input into the development of the *Digital Economy Future Directions Paper* (the Future Directions Paper) by the Department of Broadband, Communications and the Digital Economy (the Department).
7. In this submission, the Office outlines privacy considerations that it feels can be usefully incorporated into the development and drafting of the Future Directions Paper. In the Office's view, privacy and effective protection of personal information will be integral to Australia's participation in the digital economy.
8. Privacy is an issue sometimes mistakenly viewed as a barrier to harnessing the benefits of technology and the digital economy. Frequently it is placed in opposition to other desirable business goals. It is not uncommon to see 'privacy versus security' or 'privacy versus information system functionality'.<sup>1</sup> These dichotomies can erroneously encourage organisations to view privacy considerations as contrary to their business interests.
9. Many organisations also view privacy as purely a compliance issue which results in what some have called '... a somewhat low-key, 'tick the box' approach to privacy management.'<sup>2</sup>
10. Viewing privacy protection as an 'add-on' or a 'compliance issue' which is separate from system architecture and design is to significantly curtail the possibility of good information handling that could be harnessed for good effect as we embrace the digital age.
11. Privacy protections are fundamental to the success of the digital economy because without them:
  - **Personal information** is put at risk. Poor handling of personal information online may undermine individuals' trust in e-commerce and online activities.
  - **Identity management** is haphazard and risks exposing individuals to identity theft. Poor identity management can result in individuals

---

<sup>1</sup> Ann Cavoukian, Information and Privacy Commissioner of Ontario, Canada, makes this point in *Privacy and Radical Pragmatism: Change the Paradigm – A White Paper*, 8 August 2008, p7.

<sup>2</sup> UK Information Commissioner's Office, *Privacy by design*, November 2008, p6, [www.ico.gov.uk/about\\_us/news\\_and\\_views/current\\_topics/privacy\\_by\\_design.aspx](http://www.ico.gov.uk/about_us/news_and_views/current_topics/privacy_by_design.aspx).

losing control over their information or having information collected about them, used and aggregated without their knowledge.

12. In this submission, the Office highlights opportunities for building privacy into digital systems. The Office also provides responses to some of the questions posed in the Paper which relate to privacy.

## The digital economy and the Privacy Act

13. As the Department notes in the consultation draft of the Future Directions Paper, Australians already enjoy a national privacy regime that regulates the handling of personal information by Commonwealth agencies and certain private sector organisations.

14. The Privacy Act provides high-level principle-based regulation that is technology neutral. This regulation is primarily codified in 11 Information Privacy Principles (IPPs) for the Commonwealth and ACT public sectors, and 10 National Privacy Principles (NPPs) that apply to many private sector organisations.

15. During the Australian Law Reform Commission's (ALRC) recent review of privacy, the Office made submissions recommending that the Privacy Act remain technology neutral; recommendations taken up in the ALRC's final report: *For your Information: Australian Privacy Law and Practice*.<sup>3</sup> This approach provides a holistic form of regulation that applies to all aspects of the personal information life-cycle, from initial collection through to retention and destruction. Such regulation can be applied to any information handling context regardless of whether information is stored electronically or in other forms, such as paper records. This structure provides a valuable regulatory base on which to build effective e-security.

16. It is the Office's view that the Privacy Act provides and will continue to provide important protections for individual privacy which will have a bearing on Australians' confidence in the digital economy.

17. However, law alone will not be adequate to ensure privacy protection and foster confidence in the digital economy. The Office believes that information privacy will be protected most effectively in the digital economy by adopting a multi-faceted approach where the Privacy Act is combined with:

- **end user empowerment** through education to ensure that individuals are able to make informed privacy decisions when participating in the digital economy and are capable of managing potentially privacy-invasive technologies such as spyware
- **technology solutions** harnessing privacy enhancing technologies which embed privacy in ICT system design and

---

<sup>3</sup> Australian Law Reform Commission, *For your information: Australian Privacy Law and Practice*, 2008, [www.austlii.edu.au/au/other/alrc/publications/reports/108/10.html#Heading41](http://www.austlii.edu.au/au/other/alrc/publications/reports/108/10.html#Heading41).

- **international agreements and initiatives between jurisdictions** to respond to the international nature of the digital economy and the flow of personal information across jurisdictions.<sup>4</sup>

18. In this submission, the Office suggests ways for these privacy solutions to be incorporated in the Government's agenda on the digital economy and in its Future Directions Paper.

## Good privacy: protecting personal information and enhancing trust

19. A key theme of this submission is 'trust' and its importance to the overall success of the digital economy. Without it, both individuals and organisations may be hesitant to take up all that the internet and digital technology have to offer.<sup>5</sup>
20. The Office submits that trust is closely linked to privacy.<sup>6</sup> Organisations with good privacy practices are likely to generate trust among their clientele, whereas poor privacy practices can destroy trust overnight, as in the case of a major data breach. Similarly, organisations themselves may be disinclined to participate in the digital economy for fear that their systems will be hacked and trust in their brand will be lost.
21. The Office notes that there is considerable concern in the community about the lack of trustworthiness of organisations that operate online. In a survey commissioned by this Office in 2007, respondents rated businesses selling over the internet the least trustworthy out of nine types of organisations. Only 17 percent of respondents believed that businesses selling on the internet were trustworthy.<sup>7</sup>
22. Moreover, 50% of respondents to the survey said they were more concerned about providing information over the internet than they were two years ago and 65% of respondents feel more concerned about providing their details online rather than in hard copy format.<sup>8</sup>
23. If Australia is to fully engage in the digital economy, organisations and other stakeholders will need to garner trust and raise the reputation of organisations operating online. They can do this by implementing strong privacy protections and good information handling practices.

---

<sup>4</sup> See Office of the Privacy Commissioner, submission to *Australian Law Reform Commission: Issues Paper 31: Review of Privacy*, February 2007, p 418, [www.privacy.gov.au/publications/submissions/alrc/c11.html](http://www.privacy.gov.au/publications/submissions/alrc/c11.html)

<sup>5</sup> Concerns about e-commerce and lack of trust by small to medium enterprises is well illustrated by the Sensis e-Business Report 2008 figures quoted in the Future Directions Consultation Paper, see p 9. Lack of trust amongst individuals is elaborated further in the paragraphs that follow.

<sup>6</sup> For a discussion on the importance of privacy to garnering client trust, see Office of the Privacy Commissioner, *Top ten privacy issues*, speech by the Commissioner to PIPA Conference 2007, Canada, p 8, [www.privacy.gov.au/news/speeches/speech\\_top-ten-priv\\_200709.pdf](http://www.privacy.gov.au/news/speeches/speech_top-ten-priv_200709.pdf).

<sup>7</sup> Office of the Privacy Commissioner, *Community Attitudes to Privacy* Wallis Consulting, 2007, p 18, [www.privacy.gov.au/business/research/index.html#1b](http://www.privacy.gov.au/business/research/index.html#1b).

<sup>8</sup> Office of the Privacy Commissioner, *Community Attitudes to Privacy* Wallis Consulting, 2007, p 61, [www.privacy.gov.au/business/research/index.html#1b](http://www.privacy.gov.au/business/research/index.html#1b).

## Embedding privacy in the digital economy

24. The Office suggests that the Department promote a 'privacy by design' approach in its Future Directions Paper. 'Privacy by design' means building privacy into every aspect of a system and at every stage of its lifetime. The Office has noted on many occasions the importance of privacy being addressed at the design stage of new projects and being built in to system architecture and the parameters governing what information is collected and what information flows are possible.<sup>9</sup>
25. The UK Information Commissioner has also noted the importance of building in privacy in a recent report which notes that this '...approach will ensure that privacy controls are stronger, simpler to implement, harder to by-pass, and totally embedded in the system's core functionality.'<sup>10</sup>
26. Two key methods for embedding privacy into digital systems are:
- using privacy enhancing technologies and
  - doing privacy impact assessments

Privacy enhancing technologies and privacy impact assessments are explained in further detail below.

### Privacy enhancing technologies

27. The Office supports the development of privacy enhancing technologies. These technologies illustrate the important role of technology in supporting privacy and e-security. They achieve this by meeting security and other objectives, while at the same time providing individuals with appropriate control and choice over how their personal information is handled.<sup>11</sup>
28. Privacy enhancing technologies tend to fall into several categories and can be aimed at individual or organisational use, for example:
- **General information security tools** such as encryption, logical access controls, use of digital certificates etc.
  - **Data separation** which refers to systems that detach identifying information from other personal information so that the privacy of the individual is protected during processing and storage of their personal information; generally only an authorised person with a digital key is able to re-identify information.<sup>12</sup>
  - **Privacy metadata** refers to information 'tags' that can be attached to personal information during processing. These tags contain additional

---

<sup>9</sup> See, for example Office of the Privacy Commissioner submission to Department of Human Services on the proposed Health and Social Services Access Card, August 2006 [www.privacy.gov.au/publications/accesscard\\_sub\\_082006.html](http://www.privacy.gov.au/publications/accesscard_sub_082006.html).

<sup>10</sup> UK Information Commissioner's Office, *Privacy by design*, November 2008, p3, [www.ico.gov.uk/about\\_us/news\\_and\\_views/current\\_topics/privacy\\_by\\_design.aspx](http://www.ico.gov.uk/about_us/news_and_views/current_topics/privacy_by_design.aspx).

<sup>11</sup> Privacy enhancing technologies are discussed in greater detail in *Privacy Enhancing Technologies: A Whitepaper for Decision Makers* and published by the Dutch Government, [www.dutchdpa.nl/downloads\\_overig/PET\\_whitebook.pdf](http://www.dutchdpa.nl/downloads_overig/PET_whitebook.pdf).

<sup>12</sup> See *Privacy Enhancing Technologies: A Whitepaper for Decision Makers* and published by the Dutch Government, [www.dutchdpa.nl/downloads\\_overig/PET\\_whitebook.pdf](http://www.dutchdpa.nl/downloads_overig/PET_whitebook.pdf).

information such as: the source of the information, the consent obtained, how it may be used and the policies to which it is subject. Personal information can also be assigned particular conditions or 'obligations' which detail the length of time that information may be retained and whether the person has given consent for the information to be disclosed to any third parties.<sup>13</sup>

- **Privacy management systems** are systems that allow individuals to find out the privacy practices or processing policies of organisations that handle personal information and see if these match their preferences. These systems can improve the transparency of the information processing for the individual.<sup>14</sup> Some examples of privacy management systems include P3P and IBM's secure perspective software. As the UK Information Commissioner has pointed out, these tools '...may also advise users of the consequences of the information processing performed leading to an improved understanding of privacy-related issues.'<sup>15</sup>
- **Anonymising tools** include tools that hide the IP address or email address of the individual. Other similar privacy enhancing technologies in this category include those that allow anonymous or pseudonymous payment where the individual purchases a pre-paid card to make payments online.<sup>16</sup> Organisations can also build in anonymity or pseudonymity options into digital systems where full identification is not necessary. With options for anonymous transacting in place, organisations will be better able to meet their obligations under the Privacy Act which require that: 'Wherever it is lawful and practicable, individuals must have the option of not identifying themselves when entering transactions with an organisation.'<sup>17</sup>

29. The Office submits that a commitment to the development and implementation of privacy enhancing technologies should form a key element of the Australian Government's work to increase effective use of networked ICT in Australia.

30. The Office therefore recommends the Department include a section on privacy enhancing technologies in its Future Directions Paper which recognises their importance to furthering Australia's participation in the digital economy.

31. Moreover, the Office recommends that the Department include examples of notable privacy enhancing technologies amongst the case studies it incorporates into the Future Directions Paper. The Office would be happy

---

<sup>13</sup> UK Information Commissioner's Office, *Privacy by design*, November 2008, p9, [www.ico.gov.uk/about\\_us/news\\_and\\_views/current\\_topics/privacy\\_by\\_design.aspx](http://www.ico.gov.uk/about_us/news_and_views/current_topics/privacy_by_design.aspx).

<sup>14</sup> *Privacy Enhancing Technologies: A Whitepaper for Decision Makers* published by the Dutch Government [www.dutchdpa.nl/downloads\\_overig/PET\\_whitebook.pdf](http://www.dutchdpa.nl/downloads_overig/PET_whitebook.pdf)

<sup>15</sup> UK Information Commissioner's Office, *Privacy by design*, November 2008, p9, [www.ico.gov.uk/about\\_us/news\\_and\\_views/current\\_topics/privacy\\_by\\_design.aspx](http://www.ico.gov.uk/about_us/news_and_views/current_topics/privacy_by_design.aspx).

<sup>16</sup> UK Information Commissioner's Office, *Privacy by design*, November 2008, p9, [www.ico.gov.uk/about\\_us/news\\_and\\_views/current\\_topics/privacy\\_by\\_design.aspx](http://www.ico.gov.uk/about_us/news_and_views/current_topics/privacy_by_design.aspx).

<sup>17</sup> National Privacy Principle 8, Schedule 3, *Privacy Act 1988*.

to work with the Department on identifying appropriate privacy enhancing technology case studies.

### **Privacy impact assessments**

32. Privacy impact assessments offer another important opportunity for building privacy into ICT systems and projects.
33. A privacy impact assessment is an assessment tool that describes in detail the personal information flows in a project, and analyses the possible privacy impacts of the project.<sup>18</sup> A privacy impact assessment may do this by helping organisations to identify when the collection of particular information is unnecessary for a given project, or where additional accountability or oversight processes may reduce privacy risks.
34. In many cases it can be useful for privacy impact assessments to be conducted by an independent expert specialising in privacy issues and the process of conducting privacy impact assessments. There are many organisations equipped to undertake this role.
35. The elements that make up a privacy impact assessment (including identification, analysis and management of privacy risks) help organisations and agencies to develop and implement good privacy practice and underpin good public policy. Privacy impact assessments also help to engender community trust in ICT proposals if the issues raised during the privacy impact assessment are responded to adequately through the proposal's development.
36. Generally, a privacy impact assessment should:
  - describe the personal information flows in a project;
  - analyse the possible privacy impacts of those flows;
  - assess the impact of the project as a whole may have on the privacy of individuals; and
  - explain how those impacts will be eliminated or minimised.
37. For large projects, conducting a privacy impact assessment may be an iterative process, with a number of privacy impact assessments done at various stages of development or as project design evolves.
38. Consultation with key stakeholders is an important part of the privacy impact assessment process. This is particularly important where large quantities of personal information are being handled or where information of particular sensitivity is involved. Consultation will generally add significant value to a privacy impact assessment and increase stakeholder and community confidence in the initiative.
39. The Office recommends the Department emphasise in the Future Directions Paper the importance of privacy impact assessments to embedding privacy protections in new ICT systems.

---

<sup>18</sup> For further information see Office of the Privacy Commissioner, *Privacy Impact Assessment Guide*, 2006 available at <http://www.privacy.gov.au/publications/pia06/index.html>.

40. Further information on privacy impact assessments can be found in the Office's Privacy Impact Assessment Guide.<sup>19</sup>

## The digital economy and international privacy initiatives

41. The Office notes that for Australia to fully harness the benefits of the digital economy, it will need to participate in cross-jurisdictional initiatives aimed at protecting privacy and encouraging trust in transborder data flows.

42. The Office supports Australia's continuing involvement in the privacy initiatives of the following international forums.

### Organisation for Economic Cooperation and Development (OECD)

43. The Office notes the Department's reference to the OECD's Seoul Declaration in the draft front section of the Future Directions Paper and the way this declaration will guide the Government's work in pursuing digital economy objectives in the next few years.

44. The OECD's Working Party on Information Security and Privacy (WPISP) develops policy options to encourage privacy protection in a networked society.<sup>20</sup> Some of WPISP's work has included looking at the future of the internet economy from a privacy and security perspective and research on the evolution and impact of malware. The Office continues to provide input into the work of WPISP and notes the Department's strong involvement in the work of WPISP including currently chairing that group.

### Asia Pacific Economic Cooperation (APEC)

45. There are also APEC initiatives aimed at protecting information privacy and maintaining information flows among APEC economies. A key initiative is the *APEC Privacy Framework*, agreed in 2004. This Framework was developed, recognising that 'The lack of consumer trust and confidence in the privacy and security of online transactions and information networks is one element that may prevent member economies from gaining all of the benefits of electronic commerce.'<sup>21</sup>

46. APEC has initiated a 'pathfinder' to implement the Framework with the APEC Data Privacy Subgroup working on a number of pathfinder projects. These projects aim to facilitate the development of a 'Cross-border Privacy Rules' (CBPR) system for the transfer of data between APEC economies, and explore options for a type of 'trust mark' system to enhance consumer confidence in electronic commerce.

47. Australia has played a key role in these APEC initiatives by chairing the APEC Data Privacy Subgroup and taking the lead on a number of the Pathfinder projects.

---

<sup>19</sup> Office of the Privacy Commissioner, *Privacy Impact Assessment Guide, 2006* available at <http://www.privacy.gov.au/publications/pia06/index.html>.

<sup>20</sup> For information on OECD WPISP, see [www.oecd.org/departement/0,3355,en\\_2649\\_34255\\_1\\_1\\_1\\_1\\_1,00.html](http://www.oecd.org/departement/0,3355,en_2649_34255_1_1_1_1_1,00.html).

<sup>21</sup> *APEC Privacy Framework*, paragraph 1.

48. Given APEC comprises 54 percent of the world GDP and 40 percent of the world's population,<sup>22</sup> the Office recommends that the Department consider referencing the ongoing work of APEC to enhance privacy protections around transborder data flows across APEC economies. Aimed at enhancing consumer confidence and thus supporting the expansion of electronic commerce, the work of APEC and other international forums is important to Australia's domestic participation in the digital economy.

### **Asia Pacific Privacy Authorities (APPA) Forum**

49. The Office also participates in the APPA Forum which meets twice yearly and includes amongst its members privacy authorities from Australian states and territories, Korea, Hong Kong, New Zealand and Canada.

50. APPA continues to work to develop cross-jurisdiction complaint handling mechanisms to enhance the options individuals have for redress in the event of a privacy issue relating to an organisation in another country or jurisdiction.

## **Responses to specific questions raised in consultation paper**

51. The comments below relate to some of the questions asked in the *Digital Economy Future Directions Consultation Paper*.

### **What markers of success can government, industry and other stakeholders establish?**

52. The Office proposes the following markers of success for the digital economy:

- Individuals and organisations are empowered to protect personal information when participating in the global digital economy.
- Individuals trust the privacy practices of Australian organisations and agencies participating in the digital economy
- Organisations undertake privacy impact assessments on new systems and expansions of existing systems thereby ensuring that privacy protections are applied to all aspects of the information lifecycle from collection, use and storage of information through to disposal or deletion.
- Privacy enhancing technologies are accessible, easy to incorporate into digital systems and therefore widely used.
- The level of trust and participation of individuals in the digital economy increases as a consequence of good privacy practices and embedded privacy protections.

---

<sup>22</sup> See APEC website [www.apec.org/apec/about\\_apec.html](http://www.apec.org/apec/about_apec.html).

## **What more can industry and other stakeholders do to address concerns about consumer privacy and online safety?**

53. In order to address concerns about consumer privacy and online safety, the Office suggests the following actions by business and government:

### **Organisations:**

- effectively protect personal information when participating in the global digital economy and apply privacy protections to all aspects of the information lifecycle (from collection of information through to disposal or destruction)
- build privacy enhancing technologies into their digital systems
- embed privacy into digital systems at the design stage rather than ‘tacking it on’ later
- pursue systems that maximise individual control over personal information
- undertake privacy impact assessments on new systems and expansions of existing systems
- build a culture of good privacy practice through policies and training that extends across all levels of the organisation from the CEO to the customer contact officer
- promote their privacy standards and privacy enhancing technologies to consumers
- audit their systems regularly and ensure privacy protections are adequate and personal information is being handled appropriately
- opt-in to coverage by the Privacy Act (if the organisation is a small business and not already covered by the Act) to demonstrate to clients that they take privacy seriously

### **Government (in partnership with the Office of the Privacy Commissioner):**

- promote research into, development of, and take-up of privacy enhancing technologies
- encourage vendors to incorporate privacy enhancing technologies into their off-the-shelf systems and promote these as selling points
- coordinate across agencies and continues to work at raising consumer awareness about how to protect personal information online
- continue to participate in the privacy initiatives of international forums such as OECD, APEC and APPA to strengthen the protection of personal information as it travels between jurisdictions.

## **What more can be done to increase trust and confidence in online transactions?**

### **Encouraging good identity management**

54. Organisations can increase consumer trust and confidence by adopting good identity management practices.<sup>23</sup>

55. Online transactions raise a number of identity management issues that may impact on privacy. Good identity management will allow identification of an individual only to the extent necessary for the transaction. Poor identity management will be overly and unnecessarily intrusive to the individual, minimise the individual's control over their personal information and possibly facilitate identity theft.

56. Some identity management issues associated with online transactions are:

- the difficulty for individuals to determine the legitimacy and good intentions of an organisation collecting their personal information online
- the possibility of hackers and identity thieves inappropriately accessing personal information while it is being transmitted or once stored
- the emerging importance of measures, such as digital certificates and public key infrastructure, to authenticate the identity of an individual to enhance security (for example, in the place of a written signature)
- how individuals may interact anonymously in online environments, yet in a way that ensures that organisations and agencies have adequate information to conduct the transaction
- how to recognise that individuals may have multiple elements to their identity, depending on, for example, whether they are acting as a customer, an employee or a member of a family and that any online transaction need only authenticate the legitimacy of such identities to the extent necessary to enable the particular interaction and
- the enhanced capacity to link personal information with other information already held or collected by electronic means.<sup>24</sup>

57. Effective identity management (including allowing options for anonymity) should be an integral element of Australia's participation in the digital economy. The Office's 2007 *Research into Community attitudes towards Privacy in Australia* indicated that most Australians are concerned about identity theft.<sup>25</sup>

58. In the Office's view, the key to ensuring identity security sits comfortably with good privacy is to avoid the unnecessary collection of personal

---

<sup>23</sup> See for example: UK Information Commissioner's Office, *Privacy by design*, November 2008, p7.

<sup>24</sup> This is also discussed in chapter 11 of the Office's submission to the ALRC issues paper 31 available at [www.privacy.gov.au/publications/submissions/alrc/c11.html#Identity](http://www.privacy.gov.au/publications/submissions/alrc/c11.html#Identity).

<sup>25</sup> Office of the Privacy Commissioner, 2007 *Research into Community attitudes towards Privacy in Australia* [www.privacy.gov.au/business/research/index.html#1b](http://www.privacy.gov.au/business/research/index.html#1b)

information. Authentication of an individual's identity, or any other characteristics of the individual, should only be conducted where necessary. The necessity of authentication may be determined by such factors as the risks associated with a given transaction or interaction. If the collection of information is for marketing purposes, the individual should be made aware of this and have an option of not providing their personal details.

59. The Office suggests there would be merit in the Department exploring options to encourage privacy-friendly identity management processes by businesses transacting online. This could include looking at technology options that allow for anonymous or pseudonymous transacting, use of 'federated identity' system architecture and other privacy enhancing technologies.<sup>26</sup>
60. The Department could also consider including examples or case studies of good identity management systems in its Future Directions Paper to highlight opportunities for enhancing participation in the digital economy. The Office would be happy to work with the Department to identify appropriate identity management systems for this purpose.

---

<sup>26</sup> See, for example, Ann Cavoukian, Information and Privacy Commissioner, Ontario, Canada, *7 Laws of Identity: The Case for Privacy-Embedded Laws of Identity in the Digital Age*, 2006, [www.ipc.on.ca/english/Resources/Discussion-Papers/Discussion-Papers-Summary/?id=470](http://www.ipc.on.ca/english/Resources/Discussion-Papers/Discussion-Papers-Summary/?id=470).