Australian Government

Office of the Privacy Commissioner

Australian Government E-security Review

Submission to the Attorney-General's Department

August 2008

Executive Summary

The Office supports the development of an e-security framework that responds appropriately and proportionately to existing and emerging e-security risks.

Effective privacy protections for information and communication technologies will both depend on, as well as support, strong e-security.

The Office proposes that privacy in the ICT context should encompass four elements:

- strong principle-based privacy legislation that is consistent across all jurisdictions in Australia, and which includes capacity for more specific regulation where warranted
- consumer empowerment, including through education and awareness of risks, protections and rights
- the promotion of privacy enhancing technologies (PETs) and technological design that builds-in privacy at the earliest stages of development and
- cross-jurisdictional co-operation which recognises the increasingly transnational nature of online information flows and the consequent risks attached.

This submission details the existing role of the Privacy Act as foundation for strong e-security, as well as opportunities for reform that would further enhance its effectiveness. These opportunities include:

- simplifying the Privacy Act by enacting a single set of privacy principles
- encouraging national consistency in privacy regulation and
- introducing obligations for agencies and organisation to notify individuals about information security breaches.

An e-security framework should recognise the important role for consumer empowerment.

The Office notes a range of initiatives that seek to promote awareness of e-security. In addition to its own work in the area, the Office has supported such initiatives as the National E-Security Week. Ensuring that various education and awareness programs are complementary and co-ordinated is important to promoting an empowered community.

The proposed national e-security framework should encourage the development and implementation of technologies that promote strong e-security while also ensuring appropriate regard for privacy.

The continued development and adoption of “Privacy enhancing Technologies”, the use of “Privacy Impact Assessments” and the implementation of privacy friendly identity management systems are some examples of specific technology related measures that could be progressed.

International cross-jurisdictional co-operation in promoting e-security is an important objective. Forums such as the Asia Pacific Privacy Authorities, the OCED's Working Party of Information Security and Privacy (WPISP) and work done by APEC economies on developing an APEC privacy framework all provide tangible examples of how such an objective can be progressed.

The Office of the Privacy Commissioner

1. 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. The Office also has responsibilities under the Privacy Act in relation to credit worthiness information held by credit reporting agencies and credit providers, and personal tax file numbers used by individuals and organisations.

About this submission

2. The Office notes the broad terms of reference that have been provided for this review of e-security.[1] This submission focuses primarily on the following terms of reference:

> 2) examine current programs, arrangements and agency capabilities and capacities that contribute to e-security, including:
>
> ...
>
> c) other relevant information and communications technologies (ICT) initiatives being undertaken by the Commonwealth and by state and territory governments
>
> 3) address emerging e-security issues including:
>
> a) those resulting from technological change, including roll-out of the National Broadband Network, and
>
> b) an increasingly hostile online security environment, which does not respect traditional jurisdictional boundaries
>
> 4) consider opportunities provided by international cooperation, including engagement with similar economies and like-minded governments

3. This submission also highlights the important role played by effective privacy protections in promoting an appropriate e-security framework. In doing this, it draws on previous Office submissions to a range of inquiries and consultations, most notably to the Australian Law Reform Commission's review of privacy law in Australia.

4. While not expressly addressed in the terms of reference, an effective e-security framework should also give regard to effective and proportionate legislative and regulatory needs, including in regard to information privacy. This submission discusses such measures.

[1] As at 31 July 2008, the terms of reference for this review were available at http://www.ag.gov.au/www/agd/agd.nsf/Page/Consultationsreformsandreviews_E-SecurityReview_E-SecurityReview.

Privacy and e-security

5. The Office supports the development of an effective e-security framework that responds appropriately and proportionately to existing and emerging e-security risks. Such a framework is important to underpinning good privacy in an online environment.
6. In the Office's view, effective privacy protections for ICT are essential to promoting consumer confidence and promoting community participation. Such confidence is necessary to realise the potential benefits of new information and communication technologies.
7. Measures which promote good privacy for ICT are likely to both depend on, and simultaneously support, strong e-security. For example, the Office notes that many of the programs and measures conducted under the current E-Security National Agenda ('ESNA') are consistent with obligations established in the Privacy Act. The ESNA public policy statement describes a key priority for government as being to reduce the e-security risk to Australian Government information and communication systems.[2] Such an objective has the potential to enhance the privacy and information security of individuals, businesses, communities and organisations.

A framework for effective privacy in an online world

8. The Office has also discussed its views on privacy and e-security in its submissions made to the Australian Law Reform Commission's review of privacy law. The final report of this review is scheduled to be released on 11 August 2008.
9. In its submission to the ALRC's Issues Paper number 31, the Office proposed that an effective model for privacy in an online environment should encompass four elements:[3]

    - strong principle-based privacy legislation that is consistent across all jurisdictions in Australia, and which includes capacity for more specific regulation where warranted
    - consumer empowerment, including through education and awareness of risks, protections and rights
    - the promotion of privacy enhancing technologies (PETs) and technological design that builds-in privacy at the earliest stages of development and
    - cross-jurisdictional co-operation which recognises the increasingly transnational nature of online information flows and the consequent risks attached.

[2] See E-Security National Agenda Public Policy Statement at http://www.dcita.gov.au/communications_for_consumers/security/e-security

[3] See chapter 11, available at http://www.privacy.gov.au/publications/submissions/alrc/c11.html.

10. These four elements and examples of how they are currently being progressed, as well as opportunities to promote them further, are discussed in this submission.

Legislative and regulatory solutions for privacy and e-security

The Privacy Act as a regulatory foundation for e-security

11. The Privacy Act provides high-level principle-based regulation that is technologically-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.

12. The effect of this regulation is to create general rules for the handling of personal information. This includes how personal information may be collected, used, disclosed and stored. In addition, each set of principles create rights for individuals to access personal information about them and, where necessary, have it corrected.

13. In its submission to the ALRC's Discussion Paper 72, the Office has supported the Privacy Act remaining technologically-neutral. This approach provides an 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.

14. In addition, the Office notes that many Australian Government agencies are subject to agency-specific legislative requirements that add further privacy protections (such as secrecy provisions), as well as other requirements which apply more generally across government. Such measures appropriately provide protections in addition to those in the Privacy Act where privacy and security risks are greater.

Existing security provisions of the Privacy Act

15. In providing principles which address all elements of the information lifecycle, the Privacy Act includes specific obligations for the secure handling of personal information.

16. Relevantly, IPP 4 establishes obligations on agencies to have in place security safeguards, as are reasonable in the circumstances, to protect personal information against loss, unauthorised access, use, modification or disclosure, and against other misuse.

17. The Privacy Act also imposes similar, though not identical, obligations on many private sector organisations. NPP 4 requires organisations to take reasonable steps to protect personal information from misuse and loss and from unauthorised access, modification or disclosure.

18. In both IPP 4 and NPP 4, what constitutes 'reasonable steps' to protect personal information will depend on the agency's or organisation's particular circumstances, the sensitivity of the information in question, and the harm likely to result if the information is not secure.

19. Reasonable steps may include computer and network security, such as strong encryption, access controls (both physical and logical), anti-virus, spyware and malware protections, firewalls, and audit trails. Internal policies and processes, staff training and measures to promote an appropriate organisational culture may also be important elements to an effective security regime.

Opportunities to enhance privacy regulation

20. In its submission to the ALRC's inquiry into privacy law, the Office has strongly supported a number of fundamental proposals that would enhance privacy regulation in Australia and further support the e-security agenda.

Establishing a single source of obligations

21. The existing two sets of privacy principles should be consolidated to a single body of regulation that applies equally to the private sector and Australian Government agencies.[4] Such a measure would reduce regulatory complexity and promote understanding and compliance with privacy obligations.

22. Enacting a single set of privacy principles would particularly reduce complexity in the handling of personal information between government agencies and the private sector, an objective that may have particular benefits to technology and online service delivery initiatives.

National consistency in handling personal information

23. A significant issue in privacy regulation in Australia is the need for greater consistency, simplicity and clarity between jurisdictions. National consistency in privacy regulation should be a priority.[5] All states and territories should have privacy protections for their own public sectors that are consistent with the Privacy Act.

24. Such a measure would accurately reflect that personal information may flow across various levels of government and across the private sector. For example, agencies and initiatives such as CrimTrac, AUSTRAC and the proposed Document Verification Service involve the exchange of personal information across different jurisdictions. Currently, the privacy protections afforded to personal information may vary significantly as it is exchanged between jurisdictions.

25. Similarly, the Australian health system operates across all jurisdictions as well as the public and private sectors. Progress towards greater implementation of e-health, and the subsequent heightened need for

[4] See for example the Office's response to the ALRC's DP 72, proposal 3-2, available at http://www.privacy.gov.au/publications/submissions/alrc_72/PartA.html#apr4

[5] This is discussed in detail in the Office's response to the ALRC's Issues Paper 31, available at http://www.privacy.gov.au/publications/submissions/alrc/c2.html.

strong e-security in the sector, adds further support to the need for nationally consist privacy regulation.

Recognising new technologies in privacy regulation

26. While supporting the existing technology-neutral approach to privacy regulation, the Office believes that some new or emerging technologies may pose unique privacy and security challenges. Such challenges might not always be adequately addressed by technology-neutral regulation.

27. Accordingly, the Privacy Act should include provision for the making of binding rules that could apply to particular industries, technologies, agencies or organisations. These rules could introduce higher privacy protections or address matters of detail.

28. Such a mechanism is currently provided in Part IIIAA of the Privacy Act which permits private sector organisations to apply to the Privacy Commissioner to have a code approved that effectively replaces obligations under the NPP.

29. A proposal emerging from the ALRC's review is for this mechanism to be amended so that the binding codes may be made for agencies, organisations, industries or specific technologies. These codes would apply in addition to the NPPs. The Office has generally supported this approach.[6]

30. Such specific protections can assist in promoting community trust in new technologies and encourage participation and engagement in online and technology-enabled initiatives.

International transfers of personal information

31. The Office believes that personal information leaving Australia should be afforded equivalent privacy protections when it flows to a foreign jurisdiction. This need is increasingly significant where personal information can easily be transmitted and processed overseas, particularly through IT outsourcing arrangements.

32. Currently, NPP 9 generally requires organisations to take reasonable steps to ensure that the information will be afforded protections substantially similar to those in the NPPs (though there are exception to this, such as where an individual consents). No such obligation applies to Australian Government agencies.

33. The Office's submission to the ALRC's Discussion Paper 72 supported the proposal that transborder data flow protection also apply to government agencies.[7]

34. The issue of international regulatory and policy responses to online privacy and e-security is discussed in greater detail under "Promoting privacy and e-security through cross-jurisdictional co-operation" (see paragraph 65).

[6] This is discussed in detail in the Office's response to the ALRC IP31, at question 6-20 available at http://www.privacy.gov.au/publications/submissions/alrc/c6.html#L19068

[7] Part D at 392, For more information see < http://www.austlii.edu.au/au/other/alrc/publications/dp/72/ >

Notification of personal information security breaches

35. A number of overseas jurisdictions, including more than 40 US states, have responded to the risks of large scale breaches of individuals' personal information by introducing obligations on organisations to tell individuals when such breaches occur. Such measures are intended to give affected individuals the opportunity to take steps to protect their interests, such as:

    - changing government entitlement numbers
    - changing bank account details
    - being especially vigilant toward any unusual activity on credit card statements and
    - reviewing credit reporting information so as to guard against false credit applications being made in their name.

36. The Office supports the introduction of mandatory notification obligations where a breach of personal information security may pose a real risk of serious harm to an individual.[8] In addition to allowing individuals to take tangible steps to protect their interests, such a measure would promote a culture of transparency and openness in how personal information is handled.

37. In addition to providing a regulatory protection that promotes privacy and e-security, mandatory notification of breaches also empowers consumers by giving them details of how their information is handled.

38. The potential value of such an obligation was perhaps underscored by major data breaches in the United Kingdom in the last 12 months. Most notably, in November 2007, two CDs containing twenty-five million records of people claiming or receiving child benefits were lost in transit. The personal information lost included national insurance numbers and bank account details. In the following months, two UK Defence Department CDs containing the details of 600,000 defence force applicants became unaccounted for.[9]

39. These are perhaps two of the highest profile of many data breaches that have occurred internationally – for example, the US based Identity Theft Research Centre compiled a list of 448 publicly reported breaches in 2007, potentially affecting almost 128 million individuals.[10]

40. As a forerunner to any future mandatory notification obligation, the Office will be releasing during Privacy Awareness Week (24-30 August 2008) a voluntary guide to handling personal information security breaches. This

[8] This is discussed in the Office's response to chapter 47 of the ALRC's DP72 available at http://www.privacy.gov.au/publications/submissions/alrc_72/PartF.html#ach6.

[9] It has been reported that "The stolen data includes passport details, national insurance numbers, family details and doctors' addresses for people who submitted an application to the forces, the ministry said. The laptop also contained bank details for at least 3,500 people." See, *ComputerworldUK*, 20 January 2008 available at http://www.computerworlduk.com/management/security/data-control/news/index.cfm?newsid=7088.

[10] See, http://idtheftmostwanted.org/ITRC%20Breach%20Report%202007.pdf.

guide has been developed following extensive consultation and will assist agencies and organisations to determine when it is appropriate to notify affected individuals about a breach.

41. Initiatives such as this voluntary guide fall within the Office's responsibility to promote privacy through educational and guidance materials which explain obligations to agencies and organisations, while empowering individuals to understand their rights and how they can be exercised.

Promoting privacy and e-security through end user empowerment

42. In the Office's view, measures that empower end users to protect themselves in online and IT-enabled environments are essential to promoting effective privacy and e-security.

43. These measures can include promoting education and awareness of the:

- risks posed by various ICT environments and interactions
- measures that can be taken to mitigate risk, whether through technology or individual behaviour
- remedies available should something go wrong.

44. The Privacy Commissioner has a statutory function to promote the protection of individual privacy by undertaking educational programs either solely or in co-operation with other parties.[11]

45. For example, the Office promotes secure and safe online behaviour and secure information exchange by advising on social networking, online privacy tools and internet privacy.[12] Much of this advice for individuals is provided in a series of 'frequently asked questions'.[13]

46. The Office has also supported the National E-Security Awareness Week. This event is a collaborative effort between government, industry and community groups, which urges both organisations and individuals to be aware of e-security risks and how to interact securely online.[14]

47. The Office also notes initiative such as e-security education and training materials developed by the Department of Broadband, Communications and the Digital Economy (DBCDE),[15] as well work done by NetAlert,[16] and resources such as www.staysmartonline.gov.au and www.cybersmartkids.com.au (provided by the Australian Communications and Media Association).

[11] See section 27(1)(m) of the Privacy Act

[12] For more information see following links to the Office's website in regards to: FAQs on social networking www.privacy.gov.au/faqs/ypr/index.html#social_networking, Online Privacy Tools www.privacy.gov.au/internet/tools/index.html, and Protecting your privacy on the internet www.privacy.gov.au/internet_privacy/index.html

[13] The Office's 'Frequently Asked Questions' page is available at http://www.privacy.gov.au/faqs/index.html.

[14] See www.privacy.gov.au/publications/esecurity08.html

[15] More information on this initiative is available at http://www.dbcde.gov.au/communications_for_consumers/security/e-security

[16] See, http://www.netalert.gov.au/.

48. User empowerment is enhanced when individuals are aware of their rights and those right are easily accessible. The Office provides detailed guidance to individuals on how to make complaints.[17]

49. The Office submits that education and awareness programs for privacy and e-security should take into account the increasing ubiquity of ICT in many day to day transactions. Providing such material for the non-technically minded, and for individuals from non-English speaking backgrounds is important in a diverse community. For example, the Office's guidance on making complaints is accessible to individuals with non-legal or technical backgrounds and is also provided in 11 languages other than English.[18]

50. In addition, the Office suggests that there may be merit in promoting co-ordination between stakeholders in the provision of advice on e-security and privacy in an ICT context, particularly where such material deals with common issues. This would ensure consistency in the messages being provided and assist in achieving efficiency in the development and distribution of material. It would also prevent any risk that such activities might become fragmented and less effective overall.

Promoting privacy and e-security through technology and system design

51. Building and implementing technologies that promote privacy and effective e-security is essential to promoting sustainable community trust in new and emerging technologies.

52. The Office supports the development of 'Privacy Enhancing Technologies' (PETs). These technologies illustrate the potentially invaluable 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.

53. Simple examples of PET can include encryption and logical access controls, or technologies that permit the use of pseudonyms in transactions. Technologies that are often thought privacy invasive, like biometrics and smartcards, can also be implemented in privacy enhancing ways.[19]

54. The Office suggests that a commitment to the development and implementation of PETs should form an element of a national e-security framework.

[17] See http://www.privacy.gov.au/privacy_rights/complaints/index.html
[18] See http://www.privacy.gov.au/privacy_rights/languages/index.html.
[19] PETs are discussed in greater detail in Privacy Enhancing Technologies: A Whitepaper for Decision Makers and published by the Dutch Government – available at http://www.dutchdpa.nl/downloads_overig/PET_whitebook.pdf.

Privacy Impact Assessments as a tool for good e-security

55. A Privacy Impact Assessment (PIA) is an assessment tool that describes in detail the personal information flows in a project, and analyses the possible privacy impacts of the project.[20] A PIA may do this by helping an agency to identify when the collection of particular information is unnecessary for a given project, or where accountability or oversight processes may reduce privacy risks.

56. The elements that make up a PIA (including identification, analysis and management of privacy risks) help agencies to drive good privacy practice and underpin good public policy. PIAs also help to engender community trust in ICT proposals if the issues raised during the PIA are responded to adequately through the proposal's development.

57. Further information on Privacy Impact Assessments is available from the Office's draft publication, *Managing Privacy Risk - An Introductory Guide to Privacy Impact Assessment for Australian Government and ACT Government Agencies*.[21]

Identity security

58. 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 in a way that does not facilitate inappropriate or unnecessary data linkage. Bad 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.

59. Where transactions are undertaken online, additional identity management issues arise. Some issues may include:

- 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 collected online, or while it is being transmitted
- 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 can authenticate the legitimacy of 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, a constituent, a member of a family or an

[20] Further information on Privacy Impact Assessments is available from the Office's draft publication, *Managing Privacy Risk - An Introductory Guide to Privacy Impact Assessment for Australian Government and ACT Government Agencies* (available at http://www.privacy.gov.au/publications/mprdraft.pdf

[21] Available at http://www.privacy.gov.au/publications/mprdraft.pdf.

individual citizen, and that any online transaction need only authenticate the legitimacy of such identities to the extent necessary to conduct an interaction and

- the enhanced capacity to link personal information with other information already held or collected by electronic means.[22]

60. Effective identity security should be an integral element to a national e-security framework. The Office's 2007 *Research into Community attitudes towards Privacy in Australia* indicated that most Australians are concerned about identity theft.[23]

61. In this area, the Office has had ongoing involvement with the Australian Government Information Management Office (AGIMO) on the Australian Government e-Authentication Framework.

62. The Office also participates in the development of the National Identity Security Strategy ('NISS'), which provides an important cross-jurisdictional forum for the development of strong identity security and management.

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

64. The Office submits that this approach to identity security reflects an appropriate balance of risks and should form part of the proposed national e-security framework.

Promoting privacy and e-security through cross-jurisdictional co-operation

65. In the Office's view, an important component to promoting effective online privacy and e-security is to recognise the international cross-jurisdictional nature of many modern information flows. In turn, this requires international co-operation to foster good privacy outcomes for ICT.

66. The Office has recognised the importance of actively and constructively engaging with privacy and information protection regulators in other nations and economies. For example, the Office is a member of the Asia Pacific Privacy Authorities (APPA) forum. APPA membership includes similar regulators from other Australian jurisdictions, as well as New Zealand, Hong Kong, South Korea and Canada, including both the Federal Office and the province of British Columbia.[24]

67. The Office has also entered into a Memorandum of Understanding with the New Zealand Privacy Commissioner's office. The Memorandum of

[22] This is also discussed in chapter 11 of the Office's submission to the ALRC issues paper 31 available at http://www.privacy.gov.au/publications/submissions/alrc/c11.html#Identity.
[23] Office of the Privacy Commissioner, 2007 Research into Community attitudes towards Privacy in Australia < http://www.privacy.gov.au/business/research/index.html#1b >
[24] See http://www.privacy.gov.au/international/appa/index.html.

Understanding covers the sharing of information related to surveys, research projects, promotional campaigns, education and training programs, and techniques in investigating privacy violations and regulatory strategies. Other areas addressed include cooperation on complaints with a cross-border element and the possible undertaking of joint investigations.

68. The Office also actively participates in the annual International Conference of Privacy and Data Protection Authorities.[25]

Asia Pacific Economic Co-operation (APEC)

69. The Office, through the Australian Government, is an active participant in the work being progressed by the Electronic Commerce Steering Group (ECSG) of the Asia Pacific Economic Community. The primary outcome of this work has been the APEC Privacy Framework and Principles.

70. The APEC Privacy Framework aims to promote a consistent approach to information privacy protection across APEC member economies, while avoiding the creation of unnecessary barriers to information flows. The aim is to have protections consistent across the region which will assist business and member economies to be the forefront of e-commerce.

OEDC Working Party on Information Security and Privacy

71. The Office supports the work being undertaken by the Working Party on Information Security and Privacy (WPISP) convened by the Organisation for Economic Cooperation and Development (OECD).[26]

72. Among other things, this intergovernmental forum serves to develop policy options by consensus to sustain trust in the global networked society. Significantly, it also seeks to address "information security and privacy as complementary issues at the core of digital activities".[27]

73. The recent *Seoul Declaration for the Future of the Internet Economy* of 18 June 2008 is relevant to this current review of e-security.[28] Member states, including Australia, have agreed to the need to expand the availability, use, innovation and presence of competition in the internet economy, as well as:

- securing critical information infrastructures, and responding to new threats and
- ensuring the protection of personal information in the online environment.

[25] For information on these annual conferences see http://www.privacy.gov.au/links/index.html#12.

[26] See the 'security safeguards principle' in the Organisation for Economic Cooperation and Development (OECD) *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (1980) available at http://www.oecd.org/document/18/0,2340,en_2649_34255_1815186_1_1_1_1,00.html. > The *Privacy Act* was enacted to implement the OECD guidelines in Australia, as recognised in the preamble to the Act.

[27] See, "What is the Working Party on Information Security and Privacy " available at http://www.oecd.org/document/46/0,3343,en_2649_34255_36862382_1_1_1_1,00.html.

[28] The "Seoul Declaration" is available at http://www.oecd.org/document/18/0,3343,en_2649_201185_40862162_1_1_1_1,00.html.

74. Such initiatives, along with the work of other intergovernmental forums such as APEC and APPA, provide important opportunities for similar economies and like-minded governments to progress co-operation in these important areas.

75. The Office submits that the important role of these and other similar forums should form an element of any e-security framework.

An appropriate and proportionate e-security framework

76. The Office supports the development of an e-security framework, and in this submission has described a number of existing or potential initiatives that can advance such an objective in a way that simultaneously promotes good information privacy.

77. At the same time, care should be taken to ensure that any such framework retains appropriate flexibility and nuance to recognise the range of risks that may be posed by different activities and contexts.

78. By way of simple examples, IT security measures for the home user should not be so onerous as to make 'surfing the web' a 'chore' by requiring users to frequently re-enter passwords and logins. Similarly, the desire to authenticate individuals' identities by collecting personal information should be limited to where such authentication is warranted by the nature of the transaction. A highly secure online experience should not be dependent on an individual needing to reveal excessive or intrusive information about themselves.

79. Such measures could result in robust e-security, yet in poor usability and functionality, while unnecessarily lessening individuals' privacy.

80. In the Office's view, the multifaceted approach proposed in this submission provides ample opportunity for an effective and appropriate response to e-security risks. This framework of:

    - regulatory and policy solutions
    - consumer empowerment
    - privacy enhancing technology and design and
    - cross-jurisdictional co-operation

    is likely to provide a safe, secure and privacy enhancing environment that meets the needs of consumers, business and government.