Australian
Privacy
Foundation

e m a i l: enquiries@privacy.org.au
w e b : www.privacy.org.au

14 November 2011

Submission to the Department of the Prime Minister and Cabinet on the Discussion Paper "Connecting with Confidence: Optimising Australia's Digital Future"

Submission by the Australian Privacy Foundation

General issue

1. The Australian Privacy Foundation (APF) is the primary association representing the Australian public's interest in privacy. A brief backgrounder is attached.

2. We welcome the initiative of a Cyber White Paper and the September 2011 Discussion Paper preparing way for the White Paper.

3. This submission is intended to be made public.

4. We submit that, except for any justifiably confidential segments of submissions, all documents submitted should be published on the Department's web-site, and published as soon as practicable, in order to ensure that the conversation is transparent, and is not conducted behind closed doors.

About the Cyber White Paper

5. In general, the APF welcomes public attention being brought to aspects of digital citizenship, criminal activities, security and resilience, and education and skilling.

6. The APF does, however, offer the observation that the document covers a great many topics and consequently can only address them at a superficial level. The APF believes that greater progress is likely to be made through specific, more tightly defined projects.

7. The APF expresses concern about several specific aspects of the document:

- 'digital citizenship' needs to focus strongly on organisations, and not only on individuals. A major concern is the demonstrably inadequate security safeguards implemented by large numbers of organisations, the decade's delay in passing data

breach notification laws, and the urgent need for much more specific obligations in relation to data and IT security, backed up by meaningful sanctions.

- there are very few mentions of privacy within the document, and most of those are limited to a view of it as an impediment against trust and adoption.
- the paper does not recognise the considerable privacy impacts and implications of many of the measures considered in the document.
- the paper does not recognise the current realities of Internet governance, nor the debates that have been taking place about various aspects of existing institutions and processes and possible changes to governance arrangements.

8. We submit that the White Paper must:

- acknowledge the inevitability of negative impacts and implications arising from well-intentioned measures.
- recognise the vital need for designs to be subject to justification, to be proportional to the need, to be transparent, to be the subject of consultation prior to commitment being made to implementation, and to embody measures to avoid or at least mitigate negative impacts.
- identify privacy impact assessment as being the appropriate process whereby those objectives are achieved.

9. We also express concern that the civil society organisations must be directly engaged by the Department in the process of developing the White Paper, in order to ensure that public perspectives are fully appreciated, and reflected.

Privacy

10. Privacy plays a central role for all the issues raised in the Discussion Paper, such as e-health, cyber security, cyber harassment, fraud, online identity, consumer trade, intellectual property, and digital skills.

11. It must always be kept in mind that, while difficult to define, privacy is a fundamental human right protected, for example, through Article 17 of the International Covenant on Civil and Political Rights, to which Australia is a party.

12. It should also be kept in mind that, with the Internet being a near perfect tool for surveillance and monitoring, privacy must be tended with care in every decision that impacts upon it, if our fundamental human right of privacy is to be preserved in modern society.

13. Consequently, the drafting, and indeed structuring, of the Cyber White Paper must place the right of privacy at centre stage.

Improving trust in data security and use

14. The last question on page 11 of the Discussion Paper reads as follows: "How can governments improve citizens' and businesses' trust that their private data will be secured and only used for agreed purposes?"

15. Without providing a full discussion of such a complex question here, we note that the government must cater for both proactive and reactive measures. For example, there is a need for a strong proactive regulation of the circumstances under which Australian organisations are allowed to outsource data processing, or otherwise transfer personal information, to other countries. At the same time, there is a need for reactive measures such as a statutory cause of action for privacy infringements empowering victims to seek redress.[1]

16. Another important aspect of improving trust in data security and use relates to how the key concept of "consent" is applied online. As we have noted elsewhere, "While the competition is fierce, the concept of consent is probably the single most serious weakness in Australia's privacy regulation."[2]

17. The current system of Internet users consenting to the most invasive practises through the clicking of an "I agree" icon associated with a lengthy 'click-wrap agreement' that nobody seems to read is simply not working. An important task for the Cyber White Paper will be to assess and discuss the concept of consent, and online contracting through e.g. click-wrap agreements more broadly.

18. Further, considerable attention must be devoted to limiting the amount of data collected by the government, business and other organisations that individuals interact with online. Data collection must be limited to what is necessary and reasonable, and wherever possible, anonymous communications should be catered for.

---

[1] APF Submission Regarding A Statutory Cause of Action, Submission to PM&C / Attorney-General's Dept (4 Nov 2011)http://privacy.org.au/Papers/PMC-SCofAction-111104.pdf

[2] APF Submission to the Senate Standing Committee on Environment, Communications and the Arts? inquiry into the adequacy of protections for the privacy of Australians online (13 August 2010) http://www.privacy.org.au/Papers/Sen-OLP-100813.pdf.

19. In this context, it is relevant to point to the excessive data collection practice of many smart phone 'apps'. It appears almost standard for 'apps' to demand access to the users' phone records, contact lists, and indeed, locations. Such data is frequently demanded by 'apps' that do not require that type of data for their operation.

Improving consumer trust

20. Several of the questions raised in the Discussion Paper relate to consumer trust more generally, and how consumer trust in the Internet and e-commerce can be improved. One current weakness is found in the extent to which the various governmental agencies successfully enforce the law (see below). Another key weakness in Australian law is its lack of information requirements.

21. Put simply, the better informed a consumer is, the better placed (s)he is to protect her/his interests. Thus, the law should take steps to require online traders to provide more, and clearer, information about matters such as:

- information about the e-retailer;
- information about the product;
- information about the sales process;
- information about the terms of the contract;
- information about how the consumer's personal data will be dealt with; and
- information about applicable dispute resolution processes.[3]

The concept of "online identity"

22. The concept of "online identity" plays a central role in the Discussion Paper without the meaning of the concept being explained.

23. There is ample literature highlighting the difficulties of specifying the meaning of "online identity".[4] One significant task for the Cyber White Paper will be to provide a detailed discussion, and preferably a suggested definition, of the concept of "online identity". In doing so, account must be had of the question of what status IP addresses have, and will have, as a mechanism for 'identification'.

Privacy and Young People

24. The approach taken to young people is of particular importance in the context of online privacy protection. First, young people are often the earliest to adopt newly developed technologies. In that sense, they are at the forefront of online usage. Second, young people may be particularly prone to risk filled online behaviour. Finally, a change in the attitudes of the young people of today will have long term benefits not achievable in other ways.

[3] See further: D. Svantesson & R. Clarke, The *Trade Practises Act*; A Hard Act To Follow? Online Consumers and the New Australian Consumer Law Landscape (forthcoming).

[4] See e.g. D. Svantesson, A Brief Note on the CLSR 25th Anniversary Seminar - 'The Significance and Protection of Identity in the Online World', *Computer Law & Security Report* Vol. 27 Issue 1 (February 2011); pp. 1 – 3

25. Different models of the vulnerabilities, capabilities and needs of young people point to different ways of protecting their assumed interests. We suggest encouraging in young people a fundamental lifelong respect for their own and other people's privacy against unwanted intrusions from any source, including government and business as well as 'criminals'.

26. Such an approach should focus on less intrusive rather than more intrusive technical and legal measures, and adopt the emerging consensus that building individual 'resilience' and self respect in the face of any current or future challenge online is more likely to be in young people's long term interests than a series of controversial, partial, quickly obsolete and ineffective technical measures, or draconian but rarely used 'law and order' provisions.[5]

The role of intermediaries

27. Intermediaries of various kinds, such as social networking sites, play a central role in the digital economy/society. Such intermediaries can, and should, play a role in promoting responsible and accountable digital citizenship and reduce harassing and malicious online behaviour.

28. A good starting point can often be achieved by simple measures such as ensuring that default settings are reasonable.

29. At the same time, it must be recognised that society will suffer if Internet intermediaries are made to assume the role of 'judge and jury' determining what is, and is not, allowed online.

30. In this regard, a careful balance needs to be struck, and achieving such a balance ought to be one of the goals of the Cyber White Paper.

The reach of Australian law

31. While the Discussion Paper is both informative and well written in most regards, on page 9 under the heading "An Unfettered Domain" it makes an odd, and indeed misleading, statement in proclaiming that: "Most social media sites are privately owned and operated and are often based in overseas jurisdictions which may be beyond the reach of Australian law."

32. This type of statement is most unhelpful and amounts to an unwarranted declaration of bankruptcy in the legal system. It also hints at a culture of avoiding "difficult cases".

33. The reality is the Australian law in many cases has an extraterritorial reach. For example, such an extraterritoriality is clearly anticipated in s. 7 of the *Spam Act 2003* (Cth), it is found in s. 5B of the *Privacy Act 1988* (Cth) and can be implied from s. 67 of the *Australian Consumer Law* (Schedule 2 of the *Competition and Consumer Act 2010* (Cth)).

34. Thus, a soberminded consideration of the real state of things show that the problem is not so much found in the reach of Australian law. Rather the problem stems from a lacking willingness, and in some cases capacity, to enforce that law in relation to foreign-based parties.

[5] See e.g. APF Submission to the Senate Standing Committee on Legal and Constitutional Affairs regarding the inquiry into the Crimes Legislation Amendment (Sexual Offences Against Children) Bill 2010 (23 February 2010) http://www.privacy.org.au/Papers/LegCon-SexOffChn-100223.pdf.

35. Addressing these enforcement difficulties requires both further international cooperation, and a change in the mentality of key Australian enforcement agencies such as the ACCC and the Federal Privacy Commissioner.

36. Having said this, one does not have to dig particularly deep to be struck by the inadequacy of how Australian conflict of laws rules treat consumers. For example, while European e-consumers are afforded protection through the right to sue, and be sued, in their country of domicile, no similar protection is provided to Australian e-consumers.

E-Health

37. The Australian Privacy Foundation, particularly through its Health SubCommittee, has taken an active role in the discussion of e-health generally, and privacy in the context of e-health more specifically.

31. It is vital that IT be applied in order to assist in patient healthcare. There is a serious risk that interests other than those of patients may be dominating government approaches to eHealth. Many of the initiatives appear to have much more to do with the management of waste and fraud, and the availability of data for research, rather than with the treatment of patients. Another major concern is that government agencies tend to envisage monolithic structures. These are doomed to fail because of the substantial diseconomies of scale and scope that are at work in the huge and hugely complex healthcare sector. Investment must focus on facilitating inter-operability among islands, by means of standards and protocols, and not on 'grand schemes' and 'virtually centralised national database repositories'.

Concluding remarks

32. The Australian Privacy Foundation encourages the coming discussion to take place in the context of the Cyber White Paper and we look forward to, what we hope will be, a consultative approach in which public interests groups, and general society, gets to be fully involved.

For further information contact:

Vice-Chair Dr Dan Svantesson, (07) 5595 1418
E-mail: enquiries@privacy.org.au
APF Web site: http://www.privacy.org.au

Australian Privacy Foundation

Background Information

The Australian Privacy Foundation (APF) is the primary national association dedicated to protecting the privacy rights of Australians. The Foundation aims to focus public attention on emerging issues that pose a threat to the freedom and privacy of Australians. The Foundation has led the fight to defend the right of individuals to control their personal information and to be free of excessive intrusions.

The APF's primary activity is analysis of the privacy impact of systems and proposals for new systems. It makes frequent submissions to parliamentary committees and government agencies. It publishes information on privacy laws and privacy issues. It provides continual background briefings to the media on privacy-related matters.

Where possible, the APF cooperates with and supports privacy oversight agencies, but it is entirely independent of the agencies that administer privacy legislation, and regrettably often finds it necessary to be critical of their performance.

When necessary, the APF conducts campaigns for or against specific proposals. It works with civil liberties councils, consumer organisations, professional associations and other community groups as appropriate to the circumstances. The Privacy Foundation is also an active participant in Privacy International, the world-wide privacy protection network.

The APF's Board comprises professionals who bring to their work deep experience in privacy, information technology and the law.

The Board is supported by a Patron (Sir Zelman Cowen), and an Advisory Panel of eminent citizens, including former judges, former Ministers of the Crown, and a former Prime Minister.

The following pages provide access to information about the APF:

- Policies http://www.privacy.org.au/Papers/
- Resources http://www.privacy.org.au/Resources/
- Media http://www.privacy.org.au/Media/
- Current Board Members http://www.privacy.org.au/About/Contacts.html
- Patron and Advisory Panel http://www.privacy.org.au/About/AdvisoryPanel.html

The following pages provide outlines of several campaigns the APF has conducted:

- The Australia Card (1985-87)
  http://www.privacy.org.au/About/Formation.html
- CreditReporting (1988-90)
  http://www.privacy.org.au/Campaigns/CreditRpting/
- The Access Card (2006-07)
  http://www.privacy.org.au/Campaigns/ID_cards/HSAC.html
- The Media (2007-)
  http://www.privacy.org.au/Campaigns/Media/