Australian
Privacy
Foundation

http://www.privacy.org.au

Secretary@privacy.org.au

http://www.privacy.org.au/About/Contacts.html

13 August 2013

Mr Adam Redman
Head of Policy and External Affairs
Australian Computer Society Inc.

policy@acs.org.au

Dear Mr Redman

Re: Cloud Computing Consumer Protocol

The Australian Privacy Foundation (APF) is the country's leading privacy advocacy organisation. A brief backgrounder is attached.

The APF published a Policy Statement some years ago in relation to cloud computing – copy attached. This stressed the need for the following conditions to be fulfilled:

- organisational users of cloud computing take full responsibility for protection of personal data
- individual users of cloud computing products are aware of, and manage, the risks involved
- regulatory agencies ensure appropriate regulation of the technologies and practices underlying cloud computing, in ways that are not unduly intrusive or expensive

Those conditions have not been satisfied, so APF welcomes an initiative to address the problems.

However, APF expresses concern that, as envisaged in the Discussion Paper, the 'Consumer Protocol' fails to address the problems, mainly because the undertakings are merely about disclosure.

It essential that any industry code in this area:

- guides people in clarifying their own needs, and in evaluating suppliers' offerings
- involves substantive undertakings by suppliers, which address the problems

The APF supports the detailed submission by Xamax Consultancy, whose Principal is APF's Chair.

Thank you for your consideration.

Yours sincerely

David Vaile
Vice-Chair, for the Board of the APF
vicechair1@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 is open to membership by individuals and organisations who support the APF's Objects. Funding that is provided by members and donors is used to run the Foundation and to support its activities including research, campaigns and awards events.

The APF does not claim any right to formally represent the public as a whole, nor to formally represent any particular population segment, and it accordingly makes no public declarations about its membership-base. The APF's contributions to policy are based on the expertise of the members of its Board, SubCommittees and Reference Groups, and its impact reflects the quality of the evidence, analysis and arguments that its contributions contain.

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

The Board is supported by Patrons The Hon Michael Kirby and Elizabeth Evatt, 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
•	Credit Reporting (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/

Australian Privacy Foundation

APF Policy Statement re Cloud Computing

POLICY Media Resources Campaigns | About Us What Can I Do? Big Brother Contact Us

Revision of 11 November 2009

Introduction

Cloud computing is a vague term typically used to refer to a technical arrangement under which users store their data on remote servers under the control of other parties, and rely on software applications stored and perhaps executed elsewhere, rather than on their own computers. The term encompasses a variety of services, which are variously of long standing (including email), long-promised (including 'software as a service'), and relatively new.

There are many potential benefits with such arrangements. For example:

- The user can access the same set of applications, and the same data, regardless of location, and regardless of which hardware they use (such as computers, PDAs and mobile phones, including both their own hardware and devices borrowed from other individuals and organisations)
- Several users can access and share the same applications and data, which assists in collaborative work
- Backup and recovery is delegated to a service-provider, which presumably enhances its reliability
- Licensing of software and third-party data can be simplified
- Complex tasks can be performed on relatively small devices by depending on more powerful remote servers

At the same time, cloud computing is associated with severe risks in the areas of service and data integrity, consumer rights, security and privacy. This Policy Statement addresses only the APF's area of competency, privacy.

Key Concerns

The Australian Privacy Foundation has serious concerns about cloud computing:

- **Cloud Computing is an immature and obscure technology with unknown risks**. This means that:
    - **providers** of cloud computing products:
        - must undertake a Privacy Impact Assessment (PIA) before launching their product
        - must ensure that users of their products have easy access to clear and comprehensive information about the privacy and security risks involved in using the product
        - must ensure that users of their products can keep control over the use and disclosure of their personal information, including through accessible and clear privacy options
    - **user organisations** must undertake a PIA before adopting cloud computing techniques in relation to personal data, and must not use such services unless they can ensure that privacy and security risks are satisfactorily addressed, and privacy laws are complied with
    - **individuals** using cloud computing products must ensure they are aware of the privacy and security risks associated with using the product, and take those risks into account when deciding whether to use it
- In many models of cloud computing, **data may be moved outside Australia to other countries resulting in a significant loss of privacy protections**. In such cases:
    - **providers** of cloud computing products
        - must inform users of the arrangements in relation to transmission and storage of data, prior to the commencement of the service
        - must ensure that security and privacy are appropriately protected, and privacy laws complied with
        - in the case of cloud computing schemes targeted at Australians, must allow the user the choice of having personal data stored in Australia only
    - **user organisations** must ensure that privacy and security risks are satisfactorily addressed, and privacy laws complied with, and hence must not implement cloud computing techniques where the provider is unable to preclude transmission or storage in jurisdictions that do not have equivalent privacy laws
    - **individual users** of cloud computing products must carefully assess whether the use of the product justifies the risk of losing the privacy protection afforded under Australian law
- **User organisations** considering the use of cloud computing techniques for personal data **must take full responsibility** for ensuring that the service-provider:
    - applies appropriate security measures to the transmission and storage of the data – taking into account the fact that cloud computing products represent 'honey-pots' of data that inevitably attract hackers
    - does not use or disclose the data, other than as authorised by the organisation or required by law
- **Individual users** of cloud computing products **must appreciate that**:
    - network-connection may not be reliable
    - access to the service may not be reliable

  - data flows may be subject to interception, and the service-provider may fail to provide security for data transmission commensurate with its sensitivity
  - the remote data storage may be subject to unauthorised accesses – by insiders, and because cloud computing products represent 'honey pots' of data that inevitably attract hackers – and the service-provider may fail to provide security for data storage commensurate with its sensitivity
  - the service-provider may block access to or use of the data (e.g. because of a dispute over payment)
  - the service-provider may use the data for their own purposes
  - the service-provider may disclose the data
  - the service-provider may lose the data
  - the service-provider may not support extraction or transfer of the data in a format suitable to the user
- **Regulatory agencies** must take proactive steps to investigate and assess the security and privacy risks of using cloud computing, and to educate the public about these risks

Conclusions

While cloud computing has potentially valuable applications, it also gives rise to serious security and privacy risks. It is crucially important that:

- providers of cloud computing products act responsibly
- organisational users of cloud computing take full responsibility for protection of personal data
- individual users of cloud computing products be aware of the risks involved
- regulatory agencies take prompt steps to ensure appropriate, but not unduly intrusive or expensive, regulation of the technologies and practices underlying cloud computing

Resources

Cavoukian A. (2009) 'Privacy in the clouds: A white paper on privacy and digital identity' Information and Privacy Commissioner of Ontario, 2009

EPIC (2009) 'Resources on Cloud Computing' Electronic Privacy Information Center, Washington DC, 2009

Robert Gellman (2009) 'Cloud Computing and Privacy' World Privacy Forum [an industry assocation], 2009

Leslie Harris (2009) 'Perils in the Privacy Cloud' ABC News, 15 Sep 2009

Rosalie Marshall (2008) 'Experts urge caution on cloud computing' Secure Computing Magazine, 14 October 2008

Mather T., Kumaraswamy S. & Latif S. (2009) 'Cloud Security and Privacy: An Enterprise Perspective on Risks and Compliance ' O'Reilly Media, 2009

MS (2009a) 'Securing Microsoft's Cloud' Microsoft, May 2009

MS (2009b) 'Privacy in the Cloud Computing Era – A Microsoft Perspective' Microsoft, November 2009

Created: 2 September 2009 - Last Amended: 11 November 2009 by Dan Svantesson and Roger Clarke - Site Last Verified: 11 January 2009

Site Map - This document is at http://www.privacy.org.au/Papers/Media-0903.html - Privacy Policy