Australian
Privacy
Foundation

http://www.privacy.org.au

Secretary@privacy.org.au

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

16 March 2014

Dr E. Coombs
NSW Privacy Commissioner

Dear Elizabeth

Re: Guidelines for Hosting State Government Data Outside NSW Borders

We refer to the article in itNews on Friday 14 March 2014, entitled 'NSW prepares revised guide to data offshoring', at http://www.itnews.com.au/News/375068,nsw-prepares-revised-guide-to-data-offshoring.aspx. In particular, we refer to your acknowledgement that a state-specific transborder code of practice is about 13 years overdue.

APF has previously drawn the problem to attention and urged action, as the attached extracts from submissions in 2004 and 2009 attest. We accordingly applaud your stated intention to urgently prepare a code of practice, and to include within its scope the current issue of cloud computing.

We submit that it is essential that your preparatory work include consultation, if not with the public generally, then at least with relevant privacy advocacy organisations. APF is one such organisation. We draw attention to several of the APF's Policy Statements which are directly relevant to the matter, and would be pleased to assist in identifying other relevant participants:

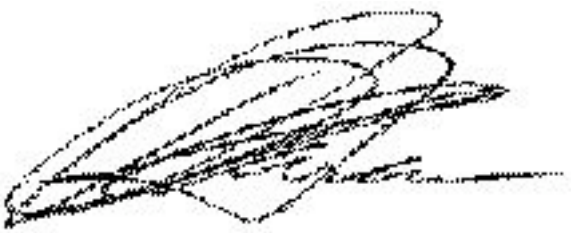
- Cloud Computing http://www.privacy.org.au/Papers/CloudComp-0911.html
- Information Security http://www.privacy.org.au/Papers/PS-Secy.html
- Data Breach Notification http://www.privacy.org.au/Papers/PS-DBN.html

We would appreciate your advice as to when and in what manner you will be conducting consultations on the draft code of practice, and look forward to the opportunity to provide a more substantial submission.

We note, however, that the present situation, in which interstate disclosures of sensitive personal information are entirely unprotected, is intolerable, and that an interim, very brief Code is necessary, in order to overcome that deficiency.

Thank you for your consideration.

Regards



Roger Clarke
Chair, for the Board of the Australian Privacy Foundation
(02) 6288 6916 Chair@privacy.org.au

Australian Privacy Foundation

Extracts from Previous Submissions

_____

Extract from APF's Submission **to NSW Attorney-General's Department, May 2004**, p.5
http://www.privacy.org.au/Papers/NSWAGsPPIPA0405.doc

Data exports

We submit that s19(2) should be brought into effect. That section only comes in to effect once a privacy code has been made under section 19(4).

Section 19(4) requires that the Privacy Commissioner prepare a privacy code of practice relating to the disclosure of personal information by public sector agencies to persons or bodies outside New South Wales, and that such code be prepared by 1 July 2001.

We understand that a draft code was prepared by the Privacy Commissioner during 2000-01, but it was not made by the Attorney General, at least partly due to uncertainty about whether "person or body who is in a jurisdiction outside New South Wales" would cover bodies such as Commonwealth Government departments which were geographically located inside NSW borders. This is a relatively minor issue which can be resolved either by a clarifying amendment, or by leaving the issue to the Courts to resolve, but should not delay introduction of the whole provision. The Commonwealth NPPs and the Victorian and Northern Territory Acts now have such provisions in force, and so should the NSW Act.

It is most unsatisfactory that s.19(2) is not in effect, particularly given that it was included at least partly to satisfy European concerns about safeguards for any personal data transferred into Australia. NSW would not want to find itself subject to restrictions on data imports from Europe because of a failure to effectively implement a 'trans-border data flow' control.

_____

Extract from the APF's letter **to the then NSW Privacy Commissioner, January 2009**
http://www.privacy.org.au/Papers/Ltr_NSWPC_ADT_case_090129.pdf

We seek an urgent explanation of your position in relation to this issue, and your advice as to your intentions with regard to making a Code under s19(4), so as to bring IPP 12 into effect, and subsequent Determinations under s19(3).

We note that s19(4) instructs the Commissioner to prepare a Code – it is not a discretion. Successive Commissioners have failed to act on this instruction, depriving the intended beneficiaries of the Act of its protection. This was always unsatisfactory, but in the context of IPP 11 not applying it is completely unacceptable, creating a major gap in the privacy protection afforded by PPIPA.

However, given that any Code prepared by you under s19 would have to be made by the Attorney-General, it may be preferable to move directly to a legislative amendment, perhaps replacing IPP 12(2)-(5) with a version of HPP 14.

_____

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

APF Policy Statement on Information Security

Organisations hold a great deal of personal data. All of it is at least to some degree sensitive, and some of it highly so. Inappropriate handling of personal data represents a threat variously to the safety, wellbeing and peace of mind of the people it relates to. Primary privacy concerns are in the areas of unauthorised use and disclosure of data, with other issues including loss of data and threats to data integrity. Personal data needs the same level of care as financial information.

The privacy interest shares a great deal of common ground with organisations' own needs for protection of data of financial and competitive value, with commercial confidentiality, and with government and national sovereignty desires for the protection of sensitive data.

Information and Information Technology Security are well-established fields of professional endeavour, supported by a substantial array of products and services and a busy industry.

Organisations have moral and legal obligations to apply the available knowledge and to thereby ensure privacy protection. This applies to:

- all government agencies at federal, State and Territory, and local levels
- large and medium-sized business enterprises and not-for-profit organisations
- small business enterprises and not-for-profit organisations that handle personal data
- service-providers, including to small organisations and consumers, where the services provided involve personal data that is under the control of the service-provider's customer (particularly personal health records and credit-card data, but also, for example, records of goods and services purchased, social media, dating services and business-contact lists)

The following, specific obligations exist, must be recognised by organisations throughout the public and private sectors, and must be enforced by regulatory agencies.

Security Governance

All organisations have obligations to:

- conduct Information Security Risk Assessment (SRA), which identifies and evaluates threats, vulnerabilities and potential harm, including a focus on risks to the privacy of individuals whose data the organisation handles
- establish an Information Security Risk Management Plan (SRMP), which specifies the information security safeguards that are to be established and maintained, including safeguards against risks to the privacy of individuals whose data the organisation handles
- establish and maintain business processes to ensure the implementation, maintenance, review and audit of those information security safeguards

Resources to guide and support these activities include:

- ISO/IEC 27005:2008 'Information technology – Security techniques – Information security risk management'
- NIST (2012) 'Guide for Conducting Risk Assessments' US National Institute for Standards and Technology, SP 800-30 Rev. 1 Sept. 2012, pp. 23-36

Security Safeguards

All organisations have obligations to establish and maintain a sufficiently comprehensive set of information security safeguards in the following areas, commensurate with the sensitivity of the data:

- Physical Access Controls, such as locks, and authorisation processes for entry to premises
- Logical Access Controls, such as user account management, privilege assignment, and user authentication
- Data Protection in Transit, such as channel encryption and authentication of devices
- Data Protection in Storage, such as access logs, backup and recovery procedures, and encryption
- Perimeter Security, such as firewalls, malware detection, and intrusion detection

- Internal Security, such as vulnerability testing, patch management, software whitelisting, malware detection, and automated detection of security incidents
- Software Security, such as pre-release testing, change control and configuration management
- Organisational Measures, such as staff training, staff supervision, separation of duties, security incident management, log monitoring and audits
- Legal Measures, such as terms of use for employees, and terms of contract for suppliers
- Data Breach Notification Processes
- Formal Audit of data protection measures

Resources to guide and support the design and implementation of effective safeguards include:

- Andress J. (2011) 'The Basics of Information Security' Syngress, www.syngress.com, 208 pp.
- Clarke R. (2013) 'Information Security for Small and Medium-Sized Organisations' Xamax Consultancy Pty Ltd, 2013
- PCI-DSS (2010) 'Payment Card Industry (PCI) Data Security Standard: Requirements and Security Assessment Procedures' Version 2.0, PCI Security Standards Council, October 2010
- ISM (2012) 'Information Security Manual – Controls' Defence Signals Directorate, 2012
- ISO/IEC 27001:2006 'Information technology — Security techniques – Information security management systems – Requirements', Annex A, pp. 13-29
- Goodrich M. & Tamassia R. (2011) 'Introduction to Computer Security' Addison-Wesley, 2011, 576 pp.

Sanctions

All organisations, and individuals within organisations, must be subject to sanctions where they fail to fulfil their information security obligations.

Sanctions must exist, and must be applied, at all of the following levels:

- civil liability by organisations
- civil liability by directors
- staff disciplinary action, up to and including dismissal in serious cases
- criminal liability for serious and repeated cases

APF Policy Statement on Data Breach Notification

A data breach occurs when personal data is exposed to an unauthorised person. It is a breach of trust by the organisation. It is commonly also a breach of the law. Unfortunately breaches of data protection laws are seldom subject to enforcement actions.

Data breaches occur remarkably frequently. Parliaments have failed to impose meaningful sanctions, and privacy oversight agencies have failed to exercise such powers and influence as they have to force organisations to ensure that appropriate security safeguards are in place.

In 2003, the Californian legislature responded to inadequacies in organisational practices by passing a Security Breach Notification Law. By 2006, 33 other US States had passed similar laws. Australian law reform has moved at glacial pace, and lags the US in this matter by a decade.

This document declares the APF's Policy on Data Breach Notification. It comprises the following sections:

- Definitions
- The Purposes of Data Breach Notification
- Organisations' Obligations in Relation to Data Security
- Organisations' Obligations in Relation to Data Breach Notification
- The Reponsibilities of the Oversight Agency
- Enforcement

Definitions

A **Data Breach** occurs where personal data held by an organisation has been subject to, or is reasonably likely to have been subject to, unauthorised access, disclosure, acquisition or loss.

A **Serious Data Breach** is a Data Breach that gives rise to a reasonable risk of harm to an individual.

A **Data Breach Notification** is a statement of the facts relating to a Data Breach.

The Purposes of Data Breach Notification

The purposes of Data Breach Notification are:

1. to inform the public, at a meaningful level of detail, about:
    - breaches
    - inadequacies in organisations' security safeguards
2. to inform individuals who have been affected by breaches, so that they can judge whether to:
    - take action to prevent or mitigate potential harm arising from the breach
    - seek compensation for harm caused
    - change their service-providers
3. to shame organisations that have seriously inadequate security safeguards into changing their ways
4. to encourage all organisations to implement adequate security safeguards

Data breach notification processes, guidelines and regulations need to be designed so as to achieve these purposes.

Organisations' Obligations in Relation to Data Security

1. All organisations must ensure that personal data is at all times subject to security safeguards commensurate with the sensitivity of the data. The APF has previously published a Policy Statement on Information Security
2. All organisations must take the steps appropriate in their particular circumstances to:

    - deter Data Breaches
    - prevent Data Breaches
    - detect Data Breaches
    - mitigate harm arising from Data Breaches; and
    - enable their investigation
3. All organisations must implement awareness, training and control measures to ensure appropriate practices by their staff
4. All organisations must conduct audits of security safeguards periodically, and when the circumstances warrant
5. All organisations must perform a Privacy Impact Assessment (PIA) when data systems are in the process of being created, and when such systems are being materially changed, in order to ensure that appropriate data protections are designed into their systems, and to demonstrate publicly that this is the case

---

Organisations' Obligations in Relation to Data Breach Notification

1. Conduct of an Investigation

Where grounds exist for suspecting that a Data Breach may have occurred, the organisation must conduct an investigation, in order to establish a sufficient understanding of the circumstances and the outcomes. The results of the investigation must be documented in a form that enables subsequent evaluation.

2. Submission of a Data Breach Notification

Where a Data Breach has occurred, or is reasonably likely to have occurred, the organisation must:

1. Submit a Data Breach Notification to the relevant oversight agency, in a manner consistent with the guidance issued by that oversight agency, as soon as practicable and without delay
2. Communicate sufficient information to affected categories of individual, the media, and/or representative and advocacy agencies, as appropriate to the circumstances

3. Form of a Data Breach Notification

A Data Breach Notification must include sufficient detail to enable the reader to achieve a proper understanding of the Data Breach, its causes, its scale, its consequences, mitigation measures, and the rights of individuals affected by it.

Details whose publication might result in harm or facilitate attacks on that or other organisations can be included within a separate Appendix whose distribution can be limited.

4. Additional Obligations in the Case of a Serious Data Breach

Where a Serious Data Breach has occurred, or is reasonably likely to have occurred, the organisation must, in addition:

1. Provide an explanation, apology and advice to each individual whose data is, or is reasonably likely to be, the subject of the Data Breach, as soon as feasible and without delay, but taking into account the possible need for a brief delay in the event that criminal investigation activities require a breathing-space
2. Publish an appropriate notice and explanation in a manner that facilitates discovery and access by people seeking the information
3. Where material harm has occurred, provide appropriate restitution
4. Inform the oversight agency of the actions taken

The Reponsibilities of the Oversight Agency

1. Publish guidance in relation to data security safeguards.
This must make clear that organisations have obligations to perform Security Risk Assessment, and to establish an Information Security Risk Management Plan whereby information security safeguards are implemented and maintained, commensurate with the sensitivity of the data

2. Publish guidance in relation to Data Breach Notifications

3. In relation to Data Breaches:

- Liaise with organisations that have suffered Data Breaches
- Facilitate the Submission of Data Breach Notifications
- Inform the Public
- Publish the Data Breach Notifications in a Public Register

4. In relation to Serious Data Breaches:

- Review the outcomes of the organisation's internal investigation
- Where doubt exists about the quality of the internal investigation, conduct its own independent investigation

- Publish the results of the review and/or investigation
- Add details of the investigation into the Public Register

5. Facilitate improvements in organisational practices relating to data security

6. Facilitate remedies for individuals who have suffered as a result of Data Breaches

---

Enforcement

All obligations in relation to Data Breach Notification must be subject to sanctions and enforcement.

The sanctions applied must reflect:

- the organisation's degree of culpability, including:
  - the extent to which the organisation had implemented safeguards commensurate with the sensitivity of the data
  - the extent to which the threat(s) and vulnerability/ies that gave rise to the Data Breach were well-known or novel
- the promptness and effectiveness with which the organisation reacted once grounds existed for suspecting that a Data Breach may have occurred
- mitigation measures adopted by the organisation once it was apparent that a Data Breach had occurred, or was reasonably likely to have occurred
- any avoidance activities, misinformation or delays by the organisation in responding to the Data Breach and in its interactions with the oversight agency
- the scale of the Data Breach
- the sensitivity of the data that was the subject of the Data Breach
- the measures undertaken by the organisation in order to address the risk of recurrence of Data Breaches (as distinct from the organisation's statements about what it intends to do)
- to the extent that financial penalties are applied, the size of the organisation

---

Created: 12 April 2013 - Last Amended: 15 April 2013 by Roger Clarke - Site Last Verified: 11 January 2009

Site Map - This document is at http://www.privacy.org.au/Directory/Page.html - Privacy Policy