Australian Government

Office of the Privacy Commissioner

Privacy and the Cloud

Speech to Cloud Computing Conference and Expo

9 September 2010

Andrew Solomon
A/g Assistant Commissioner, Operations

Good morning ladies and gentlemen. I'd like to thank the Cloud Computing Conference and Expo for the opportunity to speak to you today about cloud computing and the protection of personal information.

Overview

My discussion today primarily focuses on the type of cloud computing that involves shifting computing capabilities, such as data collection, processing or storage from the enterprise to specialist third parties, generally using the internet as the communication and delivery mechanism.

This fundamental change in the way information is collected, stored and handled by businesses and government agencies poses significant questions about how the collection and handling of personal information is appropriately undertaken in this new environment.

I'm not here today to act as a nay-sayer or to try to scare you all with worst case scenarios. Technology developments such as cloud computing can provide great opportunities to improve the way we work and these developments and the protection of personal information are reconcilable goals.

Indeed, there is a significant potential for cloud computing to enhance the protection of personal information. Stories about security breaches due to lost or stolen laptops and USB devices, or inappropriately secured enterprise computing systems abound. Storing data in the cloud, rather than on these devices or on an inadequately secured in-house system, if done well, may reduce these risks. The challenge, in order to take advantage of these new opportunities, is to ensure that personal information can be moved to a third-party service provider's facilities securely and that those facilities are also appropriately secure.

The nature of the work of a private sector organisation or government agency, the level of personal information it handles and the sensitivity of that information can all vary widely. Each organisation will have to weigh up the opportunities and risks on an individual basis.

This morning I am going to start by discussing personal information regulation in Australia including the obligations placed on most businesses and Australian Government agencies when handling personal information. I will then discuss some of the challenges of protecting personal information in a cloud computing environment and ways of identifying and mitigating those challenges.

The Privacy Act

The Australian Privacy Act is designed to regulate the collection and handling of the personal information of individuals. Personal information is defined as any

information or opinion about an individual whose identity is apparent or can reasonably be ascertained from that information. For example, a client mailing list containing names and addresses would be considered personal information for the purposes of the Act. Other items of information, eg; an ISP address or telephone number may or may not be personal information depending on the context, including the availability of connecting information.

Some personal information is also classified as sensitive information. Sensitive information includes any personal information concerning a person's race or ethnicity, their religious, political or philosophical beliefs or affiliations, and health information, including genetic information. Additional protections apply to personal information that is considered sensitive. At present, these higher protections for sensitive information only apply in the private and not for profit sectors but it is likely that proposed legislative reforms, accepted by the Australian Government last October, will extend these higher protections for sensitive information to Australian Government agencies as well.

It also important to note that Australians' concerns about the protection of personal information, and particularly the implications of technology developments on the protection of personal information, are increasing. Community attitude surveys undertaken by our Office have shown that people are becoming more concerned about the protection of personal information, especially online.[1] This means that it is very important for businesses and government agencies to get the protection of personal information right, by designing and building privacy into new technologies from the start.

In 2008 the Australian Law Reform Commission released its largest ever report: Report 108 - For Your Information; Australian Privacy Law and Practice. That report comprises approximately 3000 pages of detail about the state of privacy law in Australia and made 297 recommendations concerning the future of the protection of personal information. One of its main recommendations was that the Privacy Act should remain technology neutral. This means that the law should be principles-based and not attempt to pre- or proscribe the uses of specific technologies in relation to handling personal information. This gives the law flexibility to accommodate new developments in technology and minimises it becoming dated too quickly.

However, the Law Reform Commission also noted that organisations that use advanced technology solutions to handle personal information will need to ensure

[1] Office of the Privacy Commissioner, *Community Attitudes to Privacy 2007*, 61-2.

that they have appropriate measures in place to meet their obligations under the Privacy Act.[2]

Another of the Law Reform Commission's recommendations was that a single set of privacy principles for government and the private and not for profit sectors be introduced. At present, under the Privacy Act, Australian Government agencies are bound by the Information Privacy Principles and private and not for profit sector organisations, with some exemptions, are bound by the National Privacy Principles. The proposed combined principles, currently called the Australian Privacy Principles, in exposure draft legislation that the Senate Finance and Public Administration Committee is currently reviewing, will, if enacted, replace the two existing sets of principles and provide unified guidance for all entities in Australia that are bound by the Privacy Act.

So what are the general obligations found in the privacy principles and what are the implications of cloud computing?

Today, I'm going to focus on those principles with the greatest relevance to protecting personal information in a cloud computing environment. These concern the collection of data, the security of that data and the transfer of data outside Australia.

Data in the Cloud

There are, of course, at least two parties concerned in any cloud-computing transaction, the organisation or agency using the cloud service and the cloud service provider. One of the most basic issues that an organisation wishing to use cloud-based computing faces is maintaining control of the information once it leaves their environment and is on its way to, or in, the hands of the cloud service provider.

Our Office has produced guidelines for non-government organisations that transfer information to third party contractors. In some circumstances for the purposes of the Privacy Act a contractor may be considered to be part of the contracting organisation, in the same way that a direct employee is, but this is not usually the case. A cloud service provider would generally be considered as a separate organisation. Because of this the transfer of personal information to a contractor is generally considered to be a 'disclosure' for the purposes of the Privacy Act.[3]

---

[2] Australian Law Reform Commission, *ALRC 108: For your information: Australian Privacy Law and Practice*, 2008, paragraphs 10.9; 10.51, www.austlii.edu.au/au/other/alrc/publications/reports/108/.

[3] Office of the Privacy Commissioner, *Information Sheet (Private Sector) 8- 2001: Contractors* at www.privacy.gov.au/materials/types/infosheets/view/6567 accessed 23 August 2010.

Organisations entering into contracts that will involve the transfer of personal information need to ensure that, even if the contractor is not bound by the Privacy Act, the personal information will continue to be protected.

Cloud service providers are frequently based outside Australia and thus may not be subject to Australian legislation or it may be difficult for a regulator to enforce action against the organisation if something goes wrong. This means that it is very important that Australian organisations ensure, when they enter into a contract with a cloud service provider, that the terms of the contract enable them to continue to meet their obligations under the Privacy Act and that there is minimal risk in relation to the protection of personal information.

By its nature, cloud computing involves the virtualisation of resources such as data storage space. As information is transferred around the globe, questions arise concerning the jurisdiction over that information. This issue is probably the most complex so I think it will make more sense if I begin my discussion at the point where information is collected.

Collection

The privacy principles state that an organisation should only collect information about an individual that it needs for its functions. For an organisation or agency considering moving customer records to a cloud service provider, there is not much to worry about here if the organisation is still undertaking the collection before it is transferred to the cloud service provider as their existing systems should be in line with this principle.

The privacy principles also require that organisations and agencies inform individuals if their information will be disclosed to a third party. It is important, therefore, that individuals are informed given appropriate notice that their information will be stored in facilities provided by a third party.

Security

Data security is a crucial concern for any organisation transferring information over the internet. You'll be having a presentation on 'Security and the Cloud' later today so I'll restrict my comments on security to its implications for the protection of personal information.

Under the privacy principles, organisations and government agencies have an obligation to protect the personal information that they hold from loss or misuse and unauthorised access, modification or disclosure. The private sector principles also require organisations to take reasonable steps to ensure that any personal information that they hold is either destroyed or permanently de-identified once it is no longer needed. Under the proposed new Australian Privacy Principles, this requirement will also be extended to government agencies.

As I mentioned earlier, cloud-computing has the potential to enhance the security of information, thus aiding in the protection of personal information. For example, storing information in cloud facilities makes it centrally accessible and so, if business processes are properly designed, they can minimise the number of copies of personal information that are required within an organisation where it is spread geographically.

However, once information is stored in a cloud environment, the entity that placed it there may have less direct control over it. If a cloud-provider offers appropriate security measures, such as strong encryption of data and holding data in a purposefully designed fragmentation across servers, this can help to protect the personal information from misuse.[4] A risk occurs, however, if a cloud service provider does not offer good security measures. Organisations should ensure that cloud service providers they intend to use offer personal information security measures that are at least equal to their own and will enable them to continue to meet their obligations under the Privacy Act.[5]

We're accustomed to think about the security of our data and the need for backups and recovery strategies. But sometimes we need to be able to dispose of information securely.

As I have said, organisations have an obligation either to destroy or de-identify personal information once it is no longer needed. One of the strengths of cloud computing is its ability to offer multiple backups and help protect against data loss. This multiplication of data, however, means that it is less easy to be certain that all copies of the information have been permanently destroyed or de-identified.

The capacity of information to persist in online environments presents a challenge for managing the protection of personal information. Indeed, the CEO of Google has been quoted as predicting that, in the future, people will change their names in order to disassociate themselves from their youthful follies, all irrevocably documented online.[6] This is obviously an extreme solution and is particularly related to materials posted on social networking sites.

Data permanence does matter, however, in other contexts. For example, the Google Docs privacy policy warns that, due to their backup systems, residual copies of

---

[4] S Johnston, 'Cloud Computing and Privacy' *CircleID* 16 September 2008, www.circleid.com/posts/89163_cloud_computing_and_privacy accessed 11 Aug. 10

[5] Office of the Privacy Commissioner of Canada, *Reaching for the Cloud(s): Privacy Issues related to Cloud Computing*, priv.gc.ca/information/pub/cc_201003_e.cfm#toc5 accessed 11 August 2010.

[6] L Hearn, 'Google on Privacy: Change your name' *Sydney Morning Herald* 17 August 2010 www.smh.com.au/technology/technology-news/google-on-privacy-change-your-name-20100817-127xj.html

documents may persist for up to sixty days.[7] To give Google credit, this warning is up front and in plain language.

Organisations should question the permanence of data they move to a cloud service provider and ensure that they are able to continue to meet their obligations concerning the disposal of personal information that is no longer required.

Transborder data flows

The lifecycle of data in the cloud presents one set of concerns for the protection of personal information. Jurisdiction over that information also poses challenges. Data in the cloud may be physically stored a long way from its creators and users, potentially in overseas jurisdictions. This movement of information around the world has implications for the protection of personal information that need to be considered carefully.

Thinking around transborder data flows is by no means new. As early as 1980, the OECD *Guidelines on the Protection of Privacy and Transborder Flows of Personal Information*, which form the basis of our own Privacy Act, provided that, in developing laws and policies for the protection of personal information, member countries should not enact legislation that unnecessarily creates barriers to the movement of information.

The Law Reform Commission report I discussed earlier remains committed to this principle. It is important to protect personal information but creating excessive regulatory burdens benefits no-one.

Different jurisdictions have their own requirements concerning the movement of information across their borders. The European Union, for instance, forbids the transfer of personal information to another jurisdiction unless the protection of personal information legislation in that other jurisdiction has been assessed as 'adequate.'[8]

Other jurisdictions are less prescriptive. In Canada, organisations are required to ensure that any entity to which they transfer information can provide a 'comparable level of protection' to that in Canada.[9] The emphasis here is on the accountability of

[7] Google Docs privacy policy www.google.com/google-d-s/privacy.html accessed 17 August 2010.

[8] Australian Law Reform Commission, *ALRC 108: For your information: Australian Privacy Law and Practice*, 2008, paragraph 31.31, www.austlii.edu.au/au/other/alrc/publications/reports/108/.

[9] Office of the Privacy Commissioner of Canada, *Guidelines for Processing Personal Data across Borders*, Jan. 2009www.priv.gc.ca/information/guide/2009/gl_dab_090127_e.cfm accessed 18 August 2010.

the collecting organisation. APEC has taken a similar approach, noting the need for cooperation within a highly diverse region.[10]

In Australia, the private sector principles provide that personal information should only be allowed to pass outside Australia if the organisation believes that the recipient is subject to comparable privacy regulation or contractual terms or the individual has consented to the transfer. Under the proposed new Australian Privacy Principles, both government agencies and private organisations will remain accountable for the handling of personal information that is transferred overseas unless a series of criteria are met.

Once again, by moving information into the cloud, entities lose a degree of control over it. One issue with processing or storing information in another jurisdiction is that it may be subject to the legislation of that jurisdiction.

The implications of this were demonstrated in 2006 when it was revealed that the United States Department of the Treasury had been accessing thousands of financial records of the Society for Worldwide Interbank Financial Telecommunication (SWIFT). SWIFT itself is based in Belgium and the records accessed by the US related to transactions performed around the globe.

Our Office investigated complaints that Australians' personal information had been improperly accessed but found that we did not have jurisdiction over SWIFT's international operations. As a result of this investigation, many Australian financial institutions amended their terms and conditions for telegraphic funds transfers to include explicit consent for customers' personal information to be disclosed to overseas entities.

The Privacy Commissioner of Canada has also noted that it is impossible to prevent foreign authorities from accessing personal information held by organisations within that jurisdiction.[11]

The issue of control of information in the cloud doesn't end here. Cloud service providers are businesses themselves and may be subject to litigation. If a cloud

---

[10] Australian Law Reform Commission, *ALRC 108: For your information: Australian Privacy Law and Practice*, 2008, paragraph 31.40, www.austlii.edu.au/au/other/alrc/publications/reports/108/.

[11] Office of the Privacy Commissioner of Canada, *Responsibility of Canadian financial institutions in SWIFT's disclosure of personal information to US authorities considered* www.priv.gc.ca/cf-dc/2007/365_20070402_e.cfm E. Lictblau and J. Risen, 'Bank Data Is Sifted by U.S. in Secret to Block Terror' *The New York Times*, 23 June 2006 www.nytimes.com/2006/06/23/washington/23intel.html accessed 18 August 2010.

service provider were to have its records searched or seized as part of an investigation, personal information may be disclosed.[12]

I've already stressed the importance of strong contractual protections. Transfer of the ownership of a cloud service provider, by sale, merger or even bankruptcy, also has implications for the security of personal information held by that provider. Transfer of the cloud business may lead to changes in the terms of a cloud service. In the case of bankruptcy, the ability to retrieve personal information and dispose of copies held by the cloud service provider would partly depend on the strength of the provider's initial privacy policy.[13]

I opened this morning by saying that I'm not here simply to be negative about cloud computing. The likelihood of these scenarios affecting cloud users adversely may be remote but it is important to remember that personal information stored in the cloud can either have stronger or weaker protections than if held by an organisation itself depending on the several factors, some of which I have outlined today.

Privacy Impact Assessments

I promised earlier that I would discuss ways of mitigating risk to the protection of personal information when contemplating using cloud facilities. A tool already exists, to assist government agencies and private sector organisations to manage the implications of new projects on the protection of personal information. This tool is called a Privacy Impact Assessment. Conducting a Privacy Impact Assessment includes analysing the flow of personal information in a project and thus helps identify ways in which the protection of personal information may be affected.[14] The Assessment should highlight any potential weak points in the data life-cycle and assist in identifying ways of mitigating these weaknesses.

Poor management of personal information by a business or agency poses a number of risks to the entity as well as to the individuals whose personal information is involved.[15] The first is that the entity may not be compliant with privacy legislation. Secondly, if some misuse of personal information does occur, the resultant loss of credibility and public trust can have severe brand impact . Finally, the redesigning of systems after the event to prevent further breaches can be costly, in both time and resources, and highly disruptive.

---

[12] Office of the Privacy Commissioner of Canada, *Reaching for the Cloud(s): Privacy Issues related to Cloud Computing*, priv.gc.ca/information/pub/cc_201003_e.cfm#toc5 accessed 11 August 2010.

[13] R. Gellman, 'Privacy in the Clouds: Risks to privacy and confidentiality from cloud computing' *World Privacy Forum* 23 February 2009, 16; 20.

[14] Office of the Privacy Commissioner, 2010, *Privacy Impact Assessment Guide*, iv-v.

[15] Ibid v.

For these reasons, our Office recommends that Privacy Impact Assessments be undertaken early on in a project's initiation phase. This means that any potential weaknesses can be identified early and solutions found at the detailed design stage. In our experience, this is much more effective than trying to rectify a problem once a project is nearing implementation.

Conducting a Privacy Impact Assessment shouldn't appear as an unnecessary burden on a business that is trying to grow and develop. Rather, it should form part of the whole risk assessment process for a new undertaking and can be a valuable ongoing tool as the project progresses.

Privacy Impact Assessments are crucial if a project involves the handling of large quantities of personal information or sensitive information.[16] It is also very valuable to conduct an assessment if the project is highly innovative or represents a significant departure from previous practice. Adoption of cloud-based computing solutions is a significant innovation in processing and storing information. A Privacy Impact Assessment would, therefore, be very useful in highlighting any potential hazards and assisting an entity to appropriately protect the personal information for which it is responsible.

The assessment will provide a useful ongoing decision-making tool as the design develops and can also assist in conducting post-implementation reviews. Further, undertaking a Privacy Impact Assessment, makes a clear statement about the values of an organisation and can help to demonstrate the organisation's leadership commitment to the protection of personal information.

Our Office has produced a guide to Privacy Impact Assessments which is available on our website. We also have a list of privacy service providers on our website which would assist if you are looking to employ an external consultant to help you with the design or actually undertaking the assessment.

Conclusion

It seems fitting that we are gathered today to discuss moving computing into the clouds on the anniversary of the fixing of the first ever computer bug. This was literally a bug, or rather a moth, that was discovered lodged in a relay in the Harvard University Mark II Aiken Relay Calculator on this day in 1947.[17]

Computers and the way we undertake electronic commerce have developed exponentially from these humble beginnings. Looking forward, computing in the clouds demands detailed attention by those organisations seeking to use it and will

[16] Ibid xi.

[17] http://en.wikipedia.org/wiki/File:H96566k.jpg accessed 3 September 2010

promote greater levels of international coordination amongst privacy regulators and others as state boundaries become less significant to the transfer of information.

Our Office understands the need to balance the protection of personal information with other important goals such as innovation and business growth. With creativity and cooperation, it is always possible to achieve such aims in a privacy enhancing, rather than a privacy intrusive, way.

Thank you.