Privacy and data control in the era of cloud computing

Patrick Sefton
Principal, Brightline Lawyers
patrick.sefton@brightline.com.au

Background

Privacy law develops in response to technological change. Indeed, the opening words of the original OECD *Privacy Guidelines*[1], from which much of Australia's information privacy law has been derived, refer to privacy protection considerations necessitated by the development of "automatic data processing" (as it was then called) and the prospect of the cross-border transmission of data.

In the 30 years since those guidelines were adopted, the personal computer revolution and the dotcom bubble have each come and gone, internet and web technologies have matured and been widely deployed, broadband connectivity is available to a vast majority of businesses and households (and has a rapidly growing mobile presence), and computing, storage and network performance have each radically increased.

The purpose of this paper is to consider what appears to be a further significant and ongoing technological shift: towards so-called "cloud computing."

To avoid a debate over terms, a broad definition is taken, including within the definition of cloud computing offerings such as remote ICT managed services, utility computing and various kinds of "-as-a-service" arrangements. A working definition is given in the following section.

The paper explores the information privacy compliance and data control impacts of this technology shift, including what steps are open to clients and users of cloud computing services to maintain strong privacy compliance.

1 *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, Organisation for Economic Cooperation and Development, Paris, 1980 (adopted 23 September 1980)

What is “cloud computing”?

“Clouds” have long been used as metaphors in information and communications technology to represent abstractions of complex entities. The most prominent example is the internet itself, which is frequently represented as a cloud to abstract away the intricate technical details of how information is routed from one internet edge-point to another.[2]

More recently, cloud computing proponents have borrowed and expanded the cloud metaphor to abstract further details, particularly in the area of the provision of ICT infrastructure and software-based services. In this way the service provided, and the infrastructure used to provide it, are abstracted “into the cloud” so that a customer does not need to manage or even be aware of the details in order to take advantage of the service offering.

Many types of different services are offered on this basis. A brief explanation of the more common types of cloud services are set out below.

Data and application hosting. This is a relatively straightforward service in which an external supplier stores the customer’s data or software applications on the supplier’s ICT infrastructure. The data and applications are accessed by the client through a public or private network;

ICT Managed Services. This is an arrangement under which an organisation’s ICT service function is undertaken by a external provider. Services provided remotely might include network, desktop and security monitoring, back-up and help-desk services. Typically services are provided remotely, rather than having the provider’s personnel on site at the customer’s premises;

Application Service Provision / Software-as-a-service. Like application hosting, application service (**ASP**) and software-as-a-service (**SaaS**) providers host software applications on their own infrastructure, and provide customers with access remotely. Typically, however, an ASP or SaaS supplier is the vendor of the software application concerned, rather than a third party hosting provider. Charges for use of the software are usually on a “utility” model, that is, an ongoing periodic charge rather than an up-front licence fee;

Platform-as-a-service. This incorporates delivery of a computing platform (typically a software development platform) as a service. The advantage is that often complex

2 *The Internet Cloud*, The Industry Standard, 9 July 1999: *http://www.thestandard.com/article/0,1902,5466,00.html*

development and test environments do not have to be deployed, managed and maintained within the developer's own organisation;

Infrastructure-as-a-service. As the name suggests, this comprises delivery of ICT infrastructure as a service. Infrastructure may include servers, storage, data centre space or networking components. Again, charges are on a utility or per-use basis and can typically be scaled rapidly in response to the customer's requirements; and

Utility Computing. This is a more general term encompassing the concept that ICT products and services can be delivered on a utility basis, that is, charged on a time or usage basis and with abstraction of technical detail.

At heart, the same concept is present in each of the above types of cloud computing service. That is, that cloud computing services comprise:

- delivery of ICT capability;
- provisioned remotely and delivered as a service;
- with abstraction of technical detail.

The last point is the focus of the privacy aspects of this paper. Customers and users of cloud computing services, while taking advantage of the benefits and simplification that they offer, should take steps to ensure that privacy compliance is not ignored or abstracted with other implementation details.

Drivers for cloud services

The principal technical driver for cloud services is ubiquitous broadband. Reliable, fast internet connectivity is now available to the vast majority of organisations, and consequently cloud computing services can be rapidly and reliably delivered.

A further technical driver is the increasing prevalence of mobile computing either on small notebook computers or more recently on internet-connected portable devices such as smartphones and tablets. Portable devices are especially suited to cloud services since they are not designed to carry out intensive computing tasks, but are ideally suited to access and leverage cloud services provisioned remotely.

The primary commercial driver for organisations accessing cloud computing services is efficiency and cost reduction.[3] The costs of implementing, managing and supporting in-

3 *Cloud Computing – Survey Results*, F5 Networks, July 2009: *http://www.f5.com/pdf/reports/cloud-computing-survey-results-2009.pdf*, p9 "Needs driving the cloud"

house ICT infrastructure, including premises, skilled staff, duplication of equipment for redundancy, and aspects such as business continuity and disaster recovery, are substantial. There are significant cost-savings in contracting a cloud provider, with access to significant economies of scale and expertise, to provide that capability as part of a cloud computing service.

A further commercial driver is a reduction in capital expenditure. Since most cloud services are charged on a utility basis, there is no significant up-front capital expense involved in provisioning access to the service. The services are simply pay-as-you-go.

This also allows an organisation significant additional flexibility and agility in access to ICT solutions, platforms and infrastructure. Given utility-type charges and availability, it becomes more feasible to test applications and solutions on a trial basis, since wasted costs will be limited to the cost of the cloud service for the period of the trial. There is no significant risk of stranded capital costs.

Finally, cloud services allow for rapid provisioning of infrastructure on an "on demand" basis. For example, cloud providers claim the time to provision components such as standardised servers is now minutes (rather than the weeks it might take to order, deliver, implement and house a server under traditional procurement arrangements). On demand infrastructure also avoids the risks of over- or under-provisioning of infrastructure.

Particular examples: Microsoft

Microsoft has a cloud services product set called *Windows Azure*, though the company currently earns the significant majority of its revenue from traditionally licensed software run on customer-owned infrastructure.

On 4 March 2010, Microsoft CEO Steve Ballmer made some remarks on Microsoft's cloud computing strategy at the University of Washington.[4]

Historically, Microsoft's position on cloud computing had been one of "software plus services," that is to say, a middle ground between its traditional model, and the new approach of ICT capability delivered as cloud services.

Mr Ballmer's remarks appear to signal a change in Microsoft's approach. He made it clear that Microsoft was shifting its focus from its traditional licensing model towards cloud services, saying, "literally I will tell you we're betting our company on it," and that within a

4 *Steve Ballmer: Cloud Computing*, Microsoft News Centre, 4 March 2010, *http://www.microsoft.com/presspass/exec/steve/2010/03-04Cloud.mspx*

year 90% of Microsoft developers would be "doing things that are entirely cloud-based, or cloud inspired."

Interestingly, Microsoft has also changed its cloud services tag line from "software plus services" to "We're all in."[5] This significant change in focus from a major industry participant tends to suggest cloud services are an important technology shift.

Particular examples: Google

Google offers a number of cloud services which leverage the company's heavy investment in data centre infrastructure.

Google Apps is a cloud-based Office "workalike" service offering wordprocessing, spreadsheet, presentation graphics and email, among other services. Google charges businesses USD50 per user per year for the Apps service. Google claims at least 2 million Google Apps business clients,[6] which include the cities of Los Angeles[7] and Washington DC. Vivek Kundra, then CTO for the District of Columbia, led the effort to move Washington to Google Apps.[8] Mr Kundra has since been appointed Federal CIO in the US, and has initiated a cloud computing program at a federal level.[9]

Google also offers a platform and infrastructure service known as App Engine which allows developers to build and run web-based applications as a cloud computing service, using Google's infrastructure.

A recent technical report[10] described a Google system known as *Spanner* which spans all of Google's data centres, and moves and replicates data and computation automatically based on business rules such as cost, required latency or in response to unanticipated component failure, effectively allocating resources to tasks across Google's entire server fleet globally. One interesting aspect of the report were the design goals specified for

5 Microsoft Cloud Services home: *http://www.microsoft.com/cloud/*

6 Google Apps for Business home: *http://www.google.com/apps/intl/en/business/index.html*

7 *Los Angeles gets its Google Apps groove*, Cnet News, 20 August 2009: *http://news.cnet.com/8301-27080_3-10313846-245.html*

8 *City in the Cloud*, Government Computer News, 14 November 2008: *http://gcn.com/Articles/2008/11/14/City-in-the-cloud.aspx*

9 *NASA Ames Hosts White House CIO*, NASA, 15 September 2009: *http://www.nasa.gov/centers/ames/news/features/2009/cloud_computing.html*

10 *Designs, Lessons and Advice from Building Large Distributed Systems*, Jeff Dean, Google Fellow, 11 October 2009: *http://www.cs.cornell.edu/projects/ladis2009/talks/dean-keynote-ladis2009.pdf*

Spanner, which include management of tens of million servers (more than ten times the number Google currently operates) at thousands of locations, for billions of users. This suggests Google is preparing for very significant growth in demand for cloud services.

Privacy and data control

Clearly, privacy and data control issues are significant in the context of cloud computing services. If ICT capability is provisioned remotely as a service, this causes a loss of immediate control by the organisation over its data. If details are to be abstracted, some of those details may encompass security, privacy and data control issues. Considering customers continue to bear privacy compliance obligations, and the reputational and liability risks if privacy is breached, these issues are of particular concern for customers.

The remainder of this paper discusses the steps which can be taken to ensure that privacy compliance is not ignored or abstracted with other implementation details in a cloud services arrangement. The paper considers essential contract terms from a regulatory perspective, the enquiries which a potential customer may wish to make before entering a cloud computing arrangement, and terms which customers should consider including in contract arrangements.

Regulatory issues

There are a number of specific statutory provisions which affect service provider arrangements in the public and private sector.

Queensland public sector

In the public sector in Queensland, s35 of the Information Privacy Act[11] provides that if a service provider is providing an agency function then the agency must take all reasonable steps to ensure the service provider is required to comply with the Act (the IPPs or NPPs as applicable to the agency) as if the service provider was the agency.

Section 36 of the Act provides that a service provider which is bound by contract to comply must also under the legislation comply with the Act. This appears to be a machanism to attract the complaint and compliance mechanics of the Act.

11 *Information Privacy Act 2009* (Qld)

If the agency concerned fails to bind a service providers to comply with the Act, then s37 of the Act confirms what would apply in any case, that is, that the obligations under the Act remain with the agency concerned.

The section 35 compliance requirement is easily included in a service provider contract, and exists as an essential compliance requirement in agency contracts with service providers.

Section 33 of the Act also contains specific limitations on the cross-border transfer of personal information.

Private Sector

There are no provisions similar to s35 of the Queensland Act in the Commonwealth legislation which governs privacy compliance in the private sector.[12] Under the Commonwealth Act, a threshold question is whether the service provider is governed by the Act (or whether the provider falls within the "small business" exception to the Act because it has an annual turnover of less than three million dollars,[13] though note the effect of s6D(4)(c) and (d) concerning the application of the Act to organisations which collect or disclose personal information for payment). If a service provider is not governed, it would be preferable if the provider "opted in" to the Act.[14] The remaining alternative is to impose contract provisions which are equivalent to the requirements of the Act.

Pre-contract enquiries

Because of the substantial security, privacy and data control risks present in cloud services arrangements, suitable due diligence enquiries and risk analysis are strongly advisable before entering a services contract with a cloud computing provider.

Some of the enquiries which might be made of a potential provider are the following:

Location of provider, data. What is the legal jurisdiction of the service provider? What is/are the physical location(s) from which the service will be provided? Are they jurisdictions/locations which have strong privacy protection? Are they locations where there are significant levels of reported privacy breaches? Are there exceptions to strong privacy protection for government data collection and monitoring in

12 *Privacy Act 1988* (Cth)

13 *Privacy Act 1988* (Cth) s6C(1) & s6D

14 See *Privacy Act 1988* (Cth) s6EA

that jurisdiction / those locations? If the location is outside Australia, are statutory requirements complied with in respect of all of the kinds of data which will be managed under the service?

Backup/deletion/disposal process. Consider the lifecycle of the data under management. At what point will data be permanently deleted from the service provider's equipment (including backups). Is equipment (including backup media and devices) securely erased and destroyed once it reaches end-of-life?

Access controls. Who will have access to the data (including individuals or roles)? Are there access audit trails? If there are particular individuals who will have access to significant amounts of data (for example, database administrators) how is their access monitored and managed? Are any subcontractors involved? How is their access controlled? Is data encrypted on disk? "in flight"? Who holds access keys?

Stability / insolvency / change of supplier. Is the supplier substantial? solvent? stable? What happens if the supplier is taken over? sells the business? becomes insolvent? How easy is it to obtain a copy of all data? How easy is it to transfer to another supplier?

Single- or multi-tenanted servers. This is a technical differentiation: multi-tenanted servers reduce cost but potentially increase security risks.

Supplier's own privacy & security policies. What are the supplier's own procedures and policies? Do they include physical security? What about removal of data from premises on removable media? Does the supplier have an understanding of the role of the applicable privacy regulatory authorities, and procedures to respond to enquiries and complaints?

Reporting, notification and breach response. This is a subset of the above question about the supplier's own policies and procedures. These areas are particularly important. In particular, the supplier should have a definite policy on how it will respond to a breach in privacy.

Standards compliance. There are a number of existing and developing standards in the area of information privacy and security (summarised in a separate section below). A supplier may have certified compliance with one or more standards. A certification would usually be accompanied by an examination or audit report, which indicates departures from the certified standard. Suppliers may be asked for access to those reports (on a confidential basis).

Contract terms

Naturally, contract terms provide a critical level of protection in relation to arrangements for the provision of cloud services.

In relation to the public sector, typically ICT service acquisitions are made under the GITC[15] terms. The following section considers the existing privacy protections under those standard terms, and what may be missing.

The later section considers what specific additional terms should be included in an agreement for cloud computing services.

GITC

The GITC terms are a widely-used set of standard terms for the acquisition of ICT products and services. They are mainly used in public-sector acquisitions, but are also used by ICT procurement customers more generally. They contain the following provisions about confidentiality and information privacy.

Broad confidentiality provisions are present in GITC,[16] including obligations to maintain confidentiality and that the contractor take reasonable steps to ensure its employees and subcontractors do likewise. Importantly, the clause also provides that any confidential information must be returned on request.

The GITC terms also contain broad information privacy terms,[17] including the obligation required under s35[18] of the IPA that the supplier must comply with the relevant parts of the Act as if the supplier was the customer. The provision also expressly, albeit briefly, addresses security, use, disclosure, access and correction, and includes a provision that personal information must not be transferred outside Australia without consent.

Supporting deeds may be required to be obtained from employees and subcontractors where the customer is not reasonably satisfied that proper practices are in place.[19]

Although the GITC does address the issues of confidentiality and privacy, the terms are necessarily general and high-level. They would form a good foundation to addressing the

15 Government Information Technology Contract framework: refer to *http://www.gitc.qld.gov.au/*

16 Part 2, clause 5.4

17 Part 2, clause 5.5

18 s35 *Information Privacy Act 2009* (Qld)

19 GITC Part 2, clauses 5.4.6 (confidentiality) and 5.5.2 (privacy)

issues of privacy and data control in a cloud services contract, but should be supported by some of the more specific terms outlined below.

Suggested additional contract issues

The supplier's responses to the due diligence questions noted above should be incorporated as terms of the services contract. This includes terms addressing such areas as:

- location and jurisdiction of supplier and data;
- backup, disposal and deletion process;
- encryption and access controls;
- consequences of supplier insolvency, change of control;
- provision of / return of customer data on request, and certification of deletion from supplier's systems if the agreement is terminated. Note these rights should be very clearly expressed, since in a serious dispute they may need to be used as the basis of a mandatory injunction application to enforce the return of the data;
- assistance with transition to alternative supplier (so-called "transition out" terms) with a focus on transfer of data and continuity of service to the organisation;
- that the supplier must have, and conduct itself in accordance with, its own privacy and security policies and procedures, including DR/BC plans if applicable;
- detailed terms addressing reporting, notification and breach response; and
- a warranty that the supplier will remain certified as compliant with particular standards.

The parties may wish to reach agreement in relation to cooperation during a complaint or investigation about a privacy issue, or in respect of an access or correction request. This might include mutual notification requirements, the allocation of responsibility for managing such issues, relevant contacts within each organisation, and an escalation and dispute resolution process if a party does not comply promptly with its obligations in this area.

Preferably a cooperation arrangement referred to above should also apply to action taken in response to subpoenas and third party discovery orders to which the service provider is subject, since cloud providers make an attractive target for litigants seeking additional disclosure relating to an organisation. Along these lines, the agreement might also provide

for the service provider to assist with the customer's disclosure obligations if the customer becomes involved in litigation in which relevant documents are accessible through the cloud service.

The contract should be very clear as to the purpose for which the customer's information can be used, in particular that the provider cannot use it other than to provide services to the customer. This is, in part, to ensure that the customer can demonstrate compliance with NPP2 or IPP1 requiring collection and use only for a proper purpose.

The customer may wish to conduct (or have conducted) a periodic audit of the supplier's security and privacy processes to assure itself of continued good practice on an ongoing basis.

The customer may wish to periodically obtain a complete backup of the relevant data, if feasible, and store the backup in an alternative location. This mitigates the risk of sudden supplier insolvency or dispute leading to access issues.

Finally, there will be the issue of allocation of liability risk for a breach. Many providers will endeavour to avoid significant liability provided they have complied with their contract terms or published security procedures. Conversely, a customer will look to a provider to indemnify it against loss or damage due to a breach arising from the provider's service (including, for example, to pay any damages, the costs of remedial action and legal costs).

Ongoing management

Finally, note that privacy and security issues are not complete once a cloud services agreement has been signed. It is important to monitor and manage this kind of agreement on an ongoing basis, to ensure the supplier is maintaining compliance with the contract requirements, and to detect and deal with any issues promptly.

Such ongoing monitoring and management may include:

- periodic reporting under the contract, coupled with action to review and act on issues disclosed in such reports;
- exercise of options under the contract including arranging a compliance audit, or arranging for execution of variations or further legally binding documents (for example, the privacy deeds referred to in GITC);
- ensuring the customer has a robust internal process to address privacy breaches if and when they occur;

- co-operative & transparent management of privacy complaints and investigations;
- appropriate and timely escalation of issues given that privacy is a critical reputational & political risk;

Other issues

A customer may need to make individuals aware that information will be disclosed to a service provider as part of the customer's operations,[20] and include information its privacy policy about the existence of those arrangements.[21] Could be by way of identification of the type of organisation, or identification of the particular company.

Security standards/certifications

There are currently no specific "cloud computing" security or privacy compliance certifications. The following are the various types of security standards and certifications with which compliance may be certified in respect of providers of cloud services.

FISMA: a framework for managing information security under the US *Federal Information Security Management Act of 2002*;

HIPAA: standards for eHealth transactions under the US *Health Insurance Portability and Accountability Act of 1996* (US), extended by **HITECH**: the US *Health Information Technology for Economic and Clinical Health Act 2009*;

SOX: compliance with the requirements of the US *Sarbanes-Oxley Act of 2002* (US) (applicable to public companies) & **Basel II**: an international standard for risk management in the financial sector;

PCI DSS: This is the Payment Card Industry Data Security Standard, frequently used to certify facility or data centre security;

SAS70: This stands for Statement on Auditing Standards No.70: an accounting standard to assess internal controls within a service organisation;

ISO15489: this is an international standard for record and information management, and **ISO27001** is an international standard for information security systems.

20 NPP 1.3(d), IPP 2

21 NPP 5.2, IPP5

Conclusion

Cloud computing is a technological shift made possible by developments in communications and systems, and driven by the promise of simplification and cost reduction. Taking advantage of cloud computing may lead to significant savings for an organisation. One of the main advantages of cloud services is an abstraction of detail. Cloud service customers should take steps to ensure that important details such as privacy compliance and control of organisational data are not abstracted away from proper consideration.