Crossing Borders in the Cloud

By Phil Farrelly and Sandra Potter

***Phil Farrelly** is a director and senior technical consultant with Potter Farrelly Consulting with over 20 years experience in the support of technology solutions for law firms and courts and sits on the Executive Committee of the Victorian Society of Computers and the Law.*

***Sandra Potter** is a director of Potter Farrelly Consulting and an internationally recognized expert in the law and technology field. She is on the executive board of The Sedona Conference Working Group 6: International Electronic Information Management, Discovery and Disclosure and sits on the Executive Committee of the Victorian Society of Computers and the Law.*

Portions of this article are taken from an article prepared for the 2nd Annual Sedona Conference® International Programme on Cross-Border Discovery and Data Privacy held on 15-16 September in Washington, DC; they are reprinted courtesy of The Sedona Conference® (www.thesedonaconference.org).

Whilst there are many advances in technology in the eDiscovery area of practice, this paper attempts to discuss cloud computing and the challenges and the opportunities that cloud computing creates, although it is somewhat difficult to discern where one ends and the other begins. Advances in technology such as cloud computing present a number of challenges to cross-border discovery and data privacy. This article attempts to discuss those challenges as well.

Introduction

The Sedona Conference is using the following definition for Cloud Computing: "[A] model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction."[1]

What's in a name? Unfortunately the term "cloud" computing does little to instill confidence in the client's mind. When something has grown out of the fluffy white symbol used in most network diagrams, usually to describe the Internet, you can understand that potential users may be skeptical about how information can be securely stored and retrieved from the cloud. There is some basis for this concern because "the cloud" is a broad, inclusive term encompassing everything from the cable exiting the building to the unlimited capacity server farm sitting halfway across the globe and everything in-between. Therefore the job of processing, storing and retrieving information from such a disparate environment can throw up many challenges both technical and legal.

The cloud has been a natural evolution from past fashion represented by ASP^2 and $SaaS^3$ offerings but it is an evolution that has been more about the increasing availability of adequate low cost infrastructure rather than a development in its own right. In its simplest form it is a conduit made up of compatible pieces of infrastructure that enable the collection, processing, distribution and use of information in a way that is seamless to the user. The user simply has access to what he or she requires independent of where the application, and associated data, resides. That seamlessness however also means that difficulties can arise when it comes to identifying the definitive source of any specific information set.

Technical issues

Issues arise due to the immaturity of the market. Cloud services are the new trend and therefore new vendors are appearing everyday with a wide spread of offerings and quality available. Users who have gone down the path of engaging cloud vendors may not be fully aware of where their data is being processed or stored and are even less likely to know what technologies may be required to search and retrieve their data from the cloud based systems in the future. Typically there are a lot of

questions that only come up when problems occur but nevertheless a cloud vendor should be able to provide an infrastructure topology guide that clearly outlines the components of the provided system.

Care should also be exercised in selecting a vendor. The vendor offering the services may not actually own or operate the infrastructure being offered as there is a thriving 2nd and 3rd tier market emerging as large operators look for multiple sales channels to amortize their investment in the cloud infrastructure. While this may not be a problem if the vendor has a strong relationship with the final infrastructure provider, a user may find themselves stuck in the middle if a technical or data access issue arises.

The day-to-day performance of the system should be guaranteed by an agreed SLA[4] but the contract also needs to cover the issues of data ownership and access. Many public cloud systems will mix the one user's data with the data from other cloud clients making it very difficult to extract just one set of data from the shared database. Such extraction may affect the systems of other clients and this may limit the method and timing of any extraction that may be required. Forensic collection of such data may be very difficult if not impossible in such a system without the possibility of bringing dozens of businesses to a halt.

If the client is using a private cloud topology, where the systems are dedicated to one client, this will avoid the interruption of other businesses but may still provide challenges when it comes to accessing the data in any direct way. In fact in most cases it will be unlikely that the cloud client will have any "back-end" access to the cloud facilities as such access would be considered a very high risk by the cloud operator. Requests for information dumps will generally need to be made via the cloud operator who will then carry out the necessary work to extract the data requested (at the client's cost of course). Given the technical complexity and security built around a cloud facility it is fairly safe to say that extracting information from a cloud repository for eDiscovery purposes will have a much higher price tag than if you were extracting the same information from servers housed within the user's organization.

Other Considerations

From a process viewpoint an eDiscovery involving cloud systems will need quite a different approach to one that was contained within the user's own systems. Even putting aside the cross border issues (which hopefully have been dealt with) there is going to be more negotiation and coordination required between the cloud vendor, the client and the eDiscovery service provider.

Direct access to servers will probably not be an option for data collection so methods need to be developed and approved that will allow the extraction of data from such systems while minimizing downtime and costs.

Procedures such as a "litigation hold" may be more difficult to enforce as it may be impossible to activate the necessary controls at the "back-end" of the system.

Cross Border Issues

The cloud can effectively mask the data sources or storage repositories supporting an application used by the cloud client. A clear topology that details the storage locations is a very necessary item to ensure that the data is being stored in systems that fall within jurisdictions relevant to the sphere of operation and control as the user's own business.

If data is being stored outside the relevant, or preferred, jurisdictional control then the client will need to assess the risk and exposure associated with such a storage option. Unfortunately many cloud related decisions are based on cost and many of the low cost storage options involve jurisdictions where there could be a high exposure to risk, so this is an area where a lot of care is required. Risk here can be measured in three ways:

1. the ability to access or extract the data if required (e.g. accessing servers in Mumbai);
2. the legislative privacy regime in the jurisdiction where the data is stored; and
3. the legislative privacy regime in the jurisdiction where the client operates their business.

While a lot of focus is placed on information going in and out of Europe due to the comprehensive privacy controls that apply to most European countries any situation where data is being stored outside the assumed country of operation should be treated with care. Customers provide information to businesses with the assumption that their private data is being protected and controlled by the law of the country they live in. If an organization moves that data out of that country without the full knowledge of the customer then they could be exposing themselves to further risk if that information falls under the control of a foreign jurisdiction where that information can be used to the detriment of the customer.

As a case in point, the Gutnick defamation case (*Dow Jones and Company Inc v Gutnick* [2002] HCA 56; 210 CLR 575; 194 ALR 433; 77 ALJR 255 - December 2002) is an interesting example of information being accessed and used in a jurisdiction that was outside the control of the information owner. This however did not protect them from the consequences. While "cloud computing" wasn't even a term used in 2002, the concept of using web servers to store information has many parallels to the risks of using "sloud systems". While this was in relation to a defamation case the Judges of the High Court made some generic statements in their judgment that could easily apply to future issues that arise out of the use of cloud computing. The relevant paragraphs are as follows:

Dow Jones & Company Inc v Gutnick (HCA)
GLEESON CJ, McHUGH, GUMMOW AND HAYNE JJ.

Para 112

> "...I accept that a number of arguments support this proposition. Involved in responding to it are important questions of legal principle and policy. The proposition cannot be answered by an enquiry limited to expressions of past law. When a radically new situation is presented to the law it is sometimes necessary to think outside the square. In the present case, this involves a reflection upon the features of the Internet that are said to require a new and distinctive legal approach."

Para 113

> "First, the Internet is global. As such, it knows no geographic boundaries. Its basic lack of locality suggests the need for a formulation of new legal rules to address the absence of congruence between cyberspace and the boundaries and laws of any given jurisdiction.
>
> There are precedents for development of such new legal rules. The Law Merchant (*lex mercatoria*) arose in medieval times out of the general custom of the merchants of many nations in Europe. It emerged to respond to the growth of transnational trade. The rules of the common law of England adapted to the Law Merchant. They did so out of necessity and commonsense."

Para 114

> *"Effective legal responses*: The general principle of public international law obliging comity in legal dealings between states suggests that arguably, with respect to the legal consequences of the Internet, no jurisdiction should ordinarily impose its laws on the conduct of persons in other jurisdictions in preference to the laws that would ordinarily govern such conduct where it occurs. At least this should be so unless the former jurisdiction can demonstrate that it has a stronger interest in the resolution of the dispute in question than the latter. In conformity with this approach, the advent of the Internet suggests a need to adopt new principles, or to strengthen old ones, in responding to questions of forum or choice of law that identify, by reference to the conduct that is to be influenced, the place that has the strongest connection with, or is in the best position to control or regulate, such conduct. Normally, the laws of such a place are those most likely to be effective in securing the objectives of law, such as here, the protection of the right to free expression and access to information and the defense of reputation."

Para 123

> "Judges have adapted the common law to new technology in the past. The rules of private international law have emerged as a result of, and remain alive to, changes in the means of trans-border communication between people. The Internet's potential impact on human affairs continues to expand and is already enormous. Later judges, in a position to do so, can sometimes reformulate the law in order to keep it relevant and just. Specifically they may re-express judge-made rules that suit earlier times and different technologies."

The High Court comments bring up an interesting point, that is, it is not really important to consider where the information is stored but it is more relevant to talk about where it is used or accessed. Therefore it could be argued that data stored in Europe but only collected, processed and accessed by users and applications located in the USA falls outside the jurisdiction of the location where the data is stored. Further discussion here is out of scope but it does throw up some interesting viewpoints.

Cloud computing will no doubt throw up many challenges in technical and legal circles as the lines between ownership, control and responsibility start to blur between the players involved in the cloud. The High Court appears to acknowledge that there is a long way to go and the relevant law will continue to evolve as the use of the Internet and related technologies continues to grow.

---

[1] http://csrc.nist.gov/groups/SNS/cloud-computing/

[2] ASP – Application Service Provider

[3] SaaS – Software as a Service

[4] SLA – Service Level Agreement