

Peering Through the Cloud



Peering Through the Cloud

Cloud computing: Many benefits but there are some legal issues to consider

While outsourcing the processing or hosting of information is not a new idea, as many companies are familiar with application service providers (ASPs) and software-as-a-service (SaaS), "cloud computing" has become a catch-all phrase that represents the plethora of hosting and processing services available and delivered over the Internet.¹ The growing popularity with consumers of online services as well as the entrance of some brand-name vendors with corporate offerings (such as Amazon's Elastic Compute Cloud (EC2), Google Apps and Microsoft's recent announcement that Office 2010 will be offered as a free online service), has brought increased awareness to this combination of grid and utility computing services.² One study found that 69 per cent of Americans who use the Internet use some form of cloud computing, such as Hotmail and Gmail or online personal photo storage services.³

"...corporations and individuals are finding the siren call of cloud computing particularly compelling."

Cloud computing can be used by corporate clients to outsource, for example, data processing (such as massive database management or data mining), help desk management, CRM, word processing requirements and even all or a substantial portion of a company's IT infrastructure. Many of the above, when implemented in-house, require expensive infrastructure that are often not used at maximum efficiency. One flavour of cloud computing that may be particularly attractive to businesses engaged in sensitive industries or handling sensitive information is the "Private Cloud," whereby a business or other organization creates its own Internet-based data centre which is not generally available to the public.



Brad Newman

BUSINESS LAW - TORONTO

T: 416.216.1935

BNEWMAN@OGILVYRENAULT.COM

With vastly improved features, usability and awareness, corporations and individuals are finding the siren call of cloud computing particularly compelling. While the benefits are many, the potential legal pitfalls that come with cloud computing must be considered.

First, some of the advantages cloud computing offers:

- **Pricing:** Some cloud providers' pricing models contemplate a monthly subscription fee while other vendors provide the services on a pay-as-you-go, utility-based model. For example, users pay for the volume of data stored or number of servers required.
- **Scalability:** Cloud vendors often allocate resources to a user as needed (or requested), which has obvious benefits for both the cloud vendor and user: cloud vendors benefit greatly from economies of scale and the efficient use of their resources, while users benefit from the resulting flow-through cost savings as well as the availability, often on-demand in real-time, of vast and flexible resources that can suit their needs without having to worry about whether too much or too little was spent on in-house IT deployments.
- **Transparency:** Users can typically see exactly how much they pay for their usage of specific services, whereas non-cloud vendors would be unwilling or unable to disclose how much a user is paying for each server used or gigabyte transferred.

¹ For an overview of various cloud computing terminology and non-legal issues, see The Economist, Special Report: Let it rise (23 October 2008), online: <http://www.economist.com/specialreports/displayStory.cfm?story_id=12411882>

² Grid computing is the use of clusters of computers on a large scale to perform tasks that involve significant amounts of data and/or computer resources, while utility computing refers to the packaging of computing resources as a metered service.

³ John B. Horrigan, Cloud Computing Gains in Currency, online: Pew Research Center <<http://pewresearch.org/pubs/948/cloud-computing-gains-in-currency>>.

- **Simple Purchasing:** Though also a potential pitfall, many cloud computing services can be purchased over the Internet with a credit card and the services become available instantly. There is no need to issue a complicated request for proposal, but no opportunity to negotiate the terms of service.
- **Sensitive Data:** For businesses whose employees travel frequently and use portable laptops, the risk of loss, theft or confiscation of sensitive information stored locally on these devices can be mitigated, to some extent, by using cloud applications and storing data in the cloud.

However, all that glitters may not be gold. Companies must tread carefully when considering cloud computing as there are a variety of potential legal issues that need to be considered before engaging a cloud computing vendor:

- **Privacy:** Certain jurisdictions require personal information to remain within that jurisdiction's borders unless the receiving jurisdiction has comparable legal safeguards. For example, the EU Data Protection Directive only permits the transfer of personal data to non-EU nations that ensure "adequate level of protection"⁴. Cloud computing architecture, by its nature, provides that vendors may process resources in or through a number of jurisdictions at any given time. While in certain circumstances the cloud vendor can offer to limit where a specific user's data is held, it may not be possible or practical. Users also need to consider the possibility their data may be disclosed to the government of the jurisdiction in which their data is held by the vendor, possibly without their knowledge or consent. For example, the *USA PATRIOT Act* permits the US federal government to seek a court order for disclosure of electronic records, often without permitting notice to the user.⁵ From a Canadian perspective, a company thinking about outsourcing the processing or storage of personal information to a cloud vendor needs to consider applicable legislation—such as the *Personal Information Protection and Electronics Document Act (PIPEDA)*—which may require the company to:

a) provide notice to the data subjects their information might be stored outside of Canada and their information may be accessed by governmental authorities according to the laws of that jurisdiction;⁶ and

b) ensure the cloud vendor is contractually obligated to safeguard personal information to the same extent as the company using the cloud services.⁷ Special considerations will apply if the prospective outsourcer is a federally regulated entity and therefore would have to comply with OSFI guidelines. The OSFI guidelines specify, among other things, that an outsourcing agreement is expected to point to a physical location where the outsourced activities are to take place; this requirement could make (non-private) cloud computing impractical. Additionally, the federal *Bank Act* requires that certain records be stored in Canada.

From this brief review of just some of the potential privacy issues in cloud computing, it is apparent companies may encounter turbulence along the way.

- **Foreign Governments:** The autonomy of private or state-sponsored enterprises varies between jurisdictions. It is important for the customer to conduct due diligence and, if doubts persist about the potential for governments to monitor or access the user's systems or information flow, be sure to insist on appropriate confidentiality, security and indemnification protections or consider seeking an alternate cloud vendor.
- **Export Controls:** Given the multitude of locations from which cloud services may be provided by any one vendor, ensuring compliance with federal export controls may be difficult (where, for example, a company has sourced a software development platform in the cloud and the software to be developed contains encryption technologies subject to export controls).
- **Ownership:** Care has to be taken to ensure vendor and user rights in their respective intellectual property are clearly delineated. For example, many cloud services involve the provision of proprietary development tools by the vendor, which allows the user to create its own databases, software or other applications. In order to ensure the user comes away with a product that can be utilized by or licensed to other parties, it is essential to determine to what extent vendor or other third-party components are incorporated. Similarly, where mission critical or enterprise business processes are involved, it is critical

⁴ See Council Directive 1995/46/EC at Article 25, online: <<http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:EN:HTML>>

⁵ See Robert Gellman, *Privacy in the Clouds: Risks to Privacy and Confidentiality from Cloud Computing* (February 23, 2009): World Privacy Forum, online: <http://www.worldprivacyforum.org/pdf/WPF_Cloud_Privacy_Report.pdf>.

⁶ See Privacy Commissioner of Canada, *Outsourcing of canada.com e-mail services to US-based firm raises questions for subscribers (PIPEDA Case Summary #2008-394)*, online: <http://www.priv.gc.ca/cf-dc/2008/394_20080807_e.cfm>

⁷ See Privacy Commissioner of Canada, *Canadian-based company shares customer personal information with US parent (Case Summary #2006-333)*, online: <http://www.priv.gc.ca/cf-dc/2006/333_20060511_e.cfm>.

to ensure appropriate business continuity plans and possibly source code escrow agreements are in place to anticipate a potential bankruptcy of the vendor or some other cessation of the vendor's services.

As well, cloud vendor standard form contracts are often drafted decidedly in the cloud vendor's favour. Whether cloud computing is sourced for simple data processing or for enterprise resource planning for mission critical business processes, close attention should be paid to the following provisions commonly found in such standard form contracts—particularly if the services are going to be purchased online without any negotiation (also known as “off-the-shelf” services):

- **Uptime:** In July 2008, Amazon's S3 experienced an outage lasting more than seven hours that affected all US customers, including the high-profile social networking site Twitter.⁸ While some cloud vendors will include representations of high-levels of uptime backed by service credits issued in the event of outages (such as Amazon), other standard form contracts may provide representations of nearly guaranteed uptime while also disclaiming liability for unanticipated or unscheduled delays or outages. Where the vendor is unwilling to negotiate, companies should have their own backup systems and business continuity plans in place to address possible long-term outages by key vendors, which should contemplate redundant data storage and backup services.
- **Security:** Recently, a hacker gained access to confidential documents stored on Google Apps by hacking a Twitter employee's official email account, which was hosted by Gmail.⁹ While it should be noted that access was apparently gained by the hacker as a result of poor password selection and protection by the user, the incident serves as a reminder that sensitive information in the cloud can be vulnerable. Since vendors may not be forthcoming about their security measures and limitations of liability in their standard form agreements are often limited to the amount paid by the user or less, users may be out of luck if they suffer damages as a result of the loss or inadvertent disclosure of personal or sensitive information, or in the event of a security breach of the vendor's systems.
- **Monitoring:** Many cloud vendors' agreements include the right to monitor all data, which, without the inclusion of appropriate confidentiality and indemnification provisions, should be a source of concern for users who wish to process sensitive business information in the cloud.
- **Varying Terms:** Another common inclusion in cloud vendor standard form contracts is the ability of the vendor to modify the terms of the agreement, with such modifications deemed accepted by either continued use any time after the new terms have been posted on the vendor's website or after a certain stated time (e.g. 15 days after posting). An example of this is Apple Inc.'s recent modifications to the terms of service for its online service MobileMe. The notice provisions of the terms of service provide that notice of a change in the terms may be emailed, sent by regular mail or posted on its website. Apple recently added provisions related to its collection and use of customer information as well as adding a limitation of liability for any permanent cessation of the service.¹⁰ If Apple chose to only post these important changes to its website, they would only be noticed if the customer visited the MobileMe website, yet the changes would likely have legal effect.
- **Pay the Bills:** The services agreement of one popular cloud provides in the event a user's account falls into arrears, the vendor has the right to terminate and suspend access to the services. Perhaps most importantly, it has no obligation to retain such user's data, which may be “irretrievably deleted” after 30 days.

Conclusion

The expanding and increasingly competitive marketplace of Internet-based outsourcing services that comprise the “cloud computing” lexicon provides vendors and users with lower overall cost of implementation thanks to economies of scale and greater scalability. However, both parties must be careful to ensure their interests are protected when entering into cloud computing arrangements, particularly those cloud users purchasing off-the-shelf services subject to standard form contracts. ■

⁸ CenterNetworks, Amazon S3 Down (July 20, 2008), available online at: <<http://www.centernetworks.com/amazon-s3-down-july-2008>>.

⁹ John B. Horrigan, Cloud Computing Gains in Currency, online: Pew Research Center <<http://pewresearch.org/pubs/948/cloud-computing-gains-in-currency>>.

¹⁰ TOSBack, Apple MobileMe Terms of Service (June 18, 2009), available online at: <<http://www.tosback.org/diff.php?vid=495>>.