# Global 'Cloud' use to rise despite privacy concerns

Friday, July 5 2013

Australia today released a policy document regulating the government's use of cloud computing services. 'The cloud' is often used as shorthand for online data storage services, but the concept encompasses far more than this suggests. Most notably, it allows users to expand or decrease their usage of information technology (IT) services as and when required. This lowers overall costs, as users do not need to build the infrastructure themselves (such as servers), while injecting increased responsiveness in business operations by permitting quick expansions or reductions in service use.

## What next

The flexibility and reduced costs associated with cloud computing will continue to increase the appeal and usage of cloud services. US companies currently dominate the cloud computing market, but security and privacy concerns in the United States in particular are likely to increase support for 'national' cloud services. Therefore, European cloud providers will seek to take advantage of the EU's stronger data protection laws for marketing purposes; this could allow them to gain market share.

## Analysis

'Cloud computing' is a general term that covers a variety of software, services, and infrastructure distributed to users or subscribers over a network, usually the internet. Cloud systems are commonly used as web-based email providers, for data storage, and to synchronise data and settings across several devices. Business cloud offerings also include on-demand access to company software, databases, and networks, as well as computing power.

## Benefits of the cloud

Cloud services provide users with immediate access to their data, company services, and applications, from any location. Since cloud customers rent services and infrastructure rather than purchase them outright, the cost of IT provision is reduced: businesses pay only for the computing power, applications, or data storage that they need at that moment.

Businesses can also quickly expand their cloud IT usage if their requirements increase or decrease cloud services if demand is reduced, thereby cutting expenses. Thus, large companies can avoid the costs of building and maintaining their own data centre, and small and medium-sized enterprises (SMEs) can lower their start-up and expansion costs while remaining flexible.

Perhaps counterintuitively, cloud services can offer improved security despite the loss of direct control and an increased number of access points. Cloud providers frequently suffer attacks to their systems, so they prioritise security to ensure reliability and maintain customers' trust. Therefore, they have more sophisticated security measures -- supported by teams of security specialists -- than most companies would in an individual capacity. Even though large organisations employ dedicated security professionals to oversee their networks, SMEs could not afford this level of expertise, making cloud computing a higher security option.

Cloud providers can provide higher security

## Innate difficulties

## Impact

- Privacy and security will remain a concern, as intelligence agencies will continue to seek access to data stored with cloud providers.
- Customers will demand greater privacy protections from cloud service providers.
- In turn, this will result in increased support for comprehensive online data protection laws.
- Governments are likely to take steps towards policies covering data storage jurisdictional issues.

Nonetheless, there are innate difficulties with the cloud model. Issues of jurisdiction, access and physical control of data become increasingly pertinent as cloud use rises.

**Provider reliability**

For individuals using cloud data storage to manage their digital lives -- keeping their personal documents, photos and other media in the cloud for its low (or free) cost and convenience -- the fate of Megaupload is cautionary. In January 2012, the US Department of Justice shut down the service, accusing it of permitting file sharing of copyrighted and illegal material, and seized its US-based servers. Legitimate customers are now unable to access their content.

Complicating matters, European users' content was stored on servers based in the Netherlands. Since the shutdown, the company that owned the servers deleted all of Megaupload's (and therefore its users') data stored there. The data of legitimate personal and business Megaupload users was irretrievably lost.

**Access control**

The privacy of cloud services is another main issue, highlighted by the recent revelation of the US National Security Agency (NSA)'s PRISM programme (see INTERNATIONAL: Metadata potential sparks privacy fears - June 21, 2013). When data is stored on home computers or in company networks, the individual or business retains control over it, and any agency seeking access (usually) has to apply to that company or individual. Transferring data to the cloud means that a third party -- the cloud service provider -- also controls access to the information. As PRISM demonstrates, authorities can demand access to data directly from a third party without the owner's knowledge (see UNITED STATES: Data mining flap hits cyber policy - June 10, 2013).

**Fluid jurisdictions**

Providing services off-site and allowing remote access from any location raises inherent jurisdictional challenges. Individuals and companies could unwittingly place their data under the jurisdiction of the country in which the cloud provider's servers reside.

In an attempt to assuage non-US customers' concerns about putting their data under US jurisdiction -- and thus subject to US government demands for access under the Patriot Act -- some cloud providers built data centres in Europe and Australia for their respective customers. However, there remains the potential for companies with data centres in several jurisdictions to transfer data from one centre to another.

**Sovereign clouds?**

One proposal for taking advantage of the cloud while mitigating the privacy and jurisdictional concerns is the idea of 'national clouds'. The French government is supporting the construction of domestic cloud infrastructure, known as the 'sovereign cloud', to assure customers that their cloud data and software remains under French jurisdiction. German cloud companies are also emphasising the privacy advantage of their domestic servers.

The interest in domestic cloud providers for privacy reasons was already gaining traction pre-PRISM. Sweden's Data Inspection Board recently prevented a municipality from using cloud services from a major US provider for public services, citing concerns over the company's use of personal data. Nevertheless, use of domestic clouds does not guarantee privacy: the UK Government Communications Headquarters' alleged monitoring of communications cables and the NSA's programmes were not restricted to domestic surveillance. (Many other countries, including EU member states, have similar programmes.)

**Private clouds**

Large companies and government agencies can construct 'private clouds', in which data storage and computing power remain on-site, but services can be accessed remotely. This loses the flexibility cloud services offer and can be prohibitively expensive for smaller companies, but allows larger organisations greater control. This is especially important for regulated industries such as healthcare and financial services. Amazon currently provides members-only 'community clouds' for specialist sectors -- such as government departments or financial institutions -- for this reason. In both cases, though, the data is stored within Amazon's data centres.

Large organisations can build their own 'private clouds'

By contrast, the recent 600 million dollar deal between Amazon and the CIA marks the arrival of the true private cloud. Amazon will build and run a modified version of its public cloud within the CIA's data centres, bringing cloud benefits to the agency without the loss of control. This goes against the established cloud philosophy of offering computing power and services over the Internet, but gives the US government greater control of its data.