Pipeline
Technology for Service Providers.
www.pipelinepub.com Volume 8, Issue 9

Data Storage in the Cloud: *Fast, Cheap and Out of Control?*

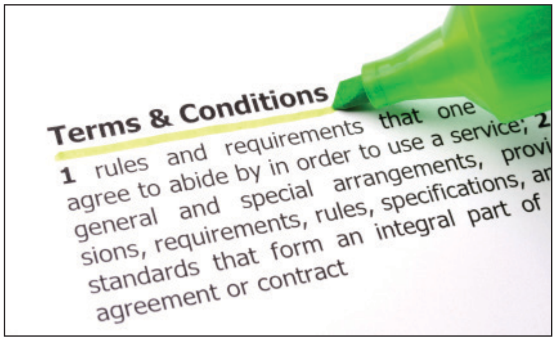
By Becky Bracken

When *South Park's* Kyle Broflovsky unknowingly agrees as part of his iTunes terms and conditions to be sewn up into a human centipede, it's funny precisely because very few people actually take the time to understand what they are agreeing to when they thoughtlessly click that little box. The completely NSFW, gross-out gag colorfully illustrates the importance of knowing what you're agreeing to, and that is certainly the case when you store data in the cloud.

Fact is, most of you would probably rather be sewn up in a human centipede than lose access to your data. Admit it. In any case, the details of a cloud computing agreement can make or break either the service provider side or the enterprise side of the equation, and protect against the unthinkable.

Salesforce.com, for instance, defines its responsibilities with this language:

"Our Responsibilities. We shall: ... (ii) use commercially reasonable efforts to make the Purchased Services available 24 hours a day, 7 days a week, except for: ... any unavailability caused by circumstances beyond Our reasonable control, including without limitation, acts of God, acts of government, floods, fires, earthquakes, civil unrest, acts of terror, strikes or other labor problems (other than those involving Our employees), Internet service provider failures or delays, or denial of service attacks..."



Terms & Conditions
1 rules and requirements that one agree to abide by in order to use a service; 2 general and special arrangements, provi sions, requirements, rules, specifications, ar standards that form an integral part of agreement or contract

It's words like "reasonable efforts," "reasonable control," and "acts of God" that leave plenty of room for interpretations and beg the question, what is reasonable? Particularly when the word "Services" means "Data" - in this case critical sales data and highly sensitive company information.

There have been several reported widespread Salesforce.com outages that left customers dead in the water and unable to access their customer data. In March 2012, a North American Salesforce.com outage left customers with little to do but take to Twitter their frustrations.

"Just thought to let you guys know that Salesforce.com is having a major outage right now!!" One customer Tweeted. "It is almost completely inaccessible, which means zero productivity for their customers, like me!!!"

When Dropbox, a file sharing service, casually announced last July they were changing their terms so that the company had the right to any files transferred over its service, it was followed by the requisite freak out from their customers.

The company wrote:

"By submitting your stuff to the Services, you grant us (and those we work with to provide the Services) worldwide, non-exclusive, royalty-free, sublicenseable rights to use, copy, distribute, prepare derivative works (such as translations or format conversions) of, perform, or publicly display that stuff to the extent reasonably necessary for the Service."

Predictably, there was a rapid about-face and the matter was dropped.

So, we're all being really, really careful with our data right? The UK's Guardian reported that a recent survey revealed only a measly 7 percent of Brits actually read the terms and conditions before they agree, even though 21 percent of respondents had suffered the consequences of agreeing to something they didn't read.

These anecdotes aren't just cautionary tales. Although the fever for public cloud computing is rising, promising cheap, innovative solutions that drive down costs, there's a real opportunity for network operators to offer a secure, more reliable alternative to cloud, and an opportunity for cloud service providers to speak to their customers in meaningful terms about the security of their data.

Where in the world is your data?

Once data is in the cloud, it can live on servers anywhere across the globe. This brings up real sticking points related to jurisdiction, should litigation become necessary. What if your data lives on the same server as company ABC and that company's data is seized by legal authorities for some reason? How can you recover your data?

Even the U.S. Department of Justice has an eye toward these types of issues related to cloud computing, particularly with rising pressure from foreign governments with respect to data security in the cloud and the unrestricted access to information provided to the US via the Patriot Act.

U.S. Ambassador Philip Verveer from the Department of Justice points out the "...the benefit of cloud computing is that is allows companies to convert capital expenditures to operating expenditures." And the government recognizes the push for companies to take advantage of the savings cloud computing offers. But because cloud is still fairly new on the scene, there has been some concern that the U.S. lacks the necessary case law to handle potential cloud disputes.

Although the fever for public cloud computing is rising, there's a real opportunity for network operators to offer a secure, more reliable alternative to cloud.

But Deputy Assistant Attorney General Bruce Swart, who is currently working with EU and other countries to develop increased cooperation in sharing data, says that the Budapest Cybercrime Convention sets a framework for access stored within a particular country and it is robust enough to cover most legal issues related to data. The treaty, passed in 2006, brings international laws into parity for increased international cooperation ferreting out criminals and accessing data. But is a loose legal framework enough?

Buyer beware

Duncan C. Card, a Toronto-based attorney with Bennett Jones, L.L.P., who specializes in cloud data ownership, takes more of a buyer beware approach. He says regardless of the technology, the cloud computing contract must consider all governance, legal, regulatory and compliance issues. This means involving general

New
Multimedia Research Center
Search OSS/BSS topics across various media types
Company Brochures, Analyst Reports, Whitepapers, Videos and more
Click here
Pipeline Research Center - Start Your Search Today!

counsel, risk management and compliance teams in addition to IT to ensure cloud computing services are a viable solution.

For instance, in October, the U.S. Securities and Exchange Commission released specific guidance related to cybersecurity breaches for publicly traded companies that calls for increased disclosure. So any company that uses a cloud computing service provider needs to ask the necessary questions to make it possible to adhere to cybersecurity disclosure requirements.

“So, is there a mechanism for reporting if a server gets hacked in Turkey?” Card asks.

But regulation doesn’t stop with security. He adds that in Canada, federal regulators prohibit financial institutions from processing data outside the country, so any cloud computing model adopted by Canadian banks would need to meet that criteria, for example.

Why the contract matters

Card underscores the inherent risk any company assumes by outsourcing key technology functions and says there is no shortcut for internal risk management and due diligence.

“Where part of a company’s IT infrastructure is provided by third parties (including outsourcing, shared services, intercompany management services, SaaS, or cloud computing) the effective execution of those services must be governed through the related service contract,” Card says. “Indeed the outsourcing or relegation of day-to-day operational duties of any IT operation or business process does not discharge the executive officers or the board from their continuing governance duties of oversight and supervision.”

Businesses that enter into a cloud computing contract should focus on outcomes and let the service provider work out the specifics of delivery and execution, for the greatest protection, according to Card. This puts all of the liability for those outcomes on the shoulders of the service provider.

“Whereas a license of software assumes the risk of that software’s possession and proper use (subject to a limited warranty term,) a service provider assumes the entire risk of acquiring and using all of the tools necessary to perform the service,” Card says. “Regardless of how your data processing services are structured, that performance risk transfers to the service provider based on the provider’s agreement to provide and deliver operational ‘results’ and outcomes.”

> **“There has been an over priority of price over risk management.”**

You get what you pay for

Cloud computing is attractive because it looks like a low-cost solution for updating infrastructure and outsourcing, but as Card points out, sometimes, “You get what you pay for.”

He adds that many cloud computing offers start out low priced, but once requirements for security and reliability are built into the agreement, the price can rise substantially. A customer who needs data stored on a secure server in California, rather than some outpost in Africa, is going to pay top dollar for that computing solution. It’s these incremental costs, once factored into the agreement, that can price some cloud computing solutions too high to justify the risk.

“Because of the recession, companies are feeling a lot more financial pressure, and cloud computing looks like an easy way to drive down costs,” Card says. “That’s understandable, but dangerous.”

He’s concerned that some businesses that adopt cloud computing to drive down costs might later regret the decision.

“In more capable economic circumstances they might revisit that approach,” Card adds. “There has been an over priority of price over risk management.”

So what does all of this mean about the future of cloud computing? Fundamentally, the model works best when dealing with low-risk, high-volume commodity computing. Once proprietary, service differentiating data enters the cloud, there are a whole host of potential risks.

Service providers too, need to assess the risk they are taking on by ensuring a certain level of service and thoughtfully consider those risks when pricing, both when adopting cloud solutions and when offering it to their customers.

The fever for cloud computing continues to rise, but with so many legal, regulatory, compliance and governance issues involved in any cloud computing agreement, it’s easy for service providers and enterprise customers alike to make critical, game changing mistakes. Cloud providers can avoid these pitfalls learning from the many mistakes made by others and by addressing the issues surrounding cloud data ownership and clearly communicating it to their customers. And for the customers, it’s still “buyer beware.”