MORRISON | FOERSTER

Legal Updates & News

Bulletins

Cloud Computing and Outsourcing: Is Data Lost in the Fog?

June 2009
by Julian S. Millstein, Matthew King

Cloud Computing and Outsourcing: Is Data Lost in the Fog?

Cloud computing is here. And if it isn't at your company yet, it soon will be. Cloud computing is simply the latest version of the historical use of technology to increase flexibility and reduce costs. By providing a bundled and scalable solution of software, infrastructure, data storage and communication, cloud computing providers allow companies to reserve cash, avoid expensive IT commitments, efficiently scale usage based on need, and launch new services quickly. However, there is truly no free lunch - at this point in its development, outsourced cloud computing fails to address important questions of legal risk associated with knowing where data is stored and transmitted. This Alert discusses several of these issues, which must be considered by companies turning to third-party cloud computing solutions.

Related Practices:

- Privacy and Data Security
- Sourcing
- Technology Transactions

First, of course, we need to define what we are talking about, because there are many definitions of "cloud computing." Recently, a CIO we know defined it as a computing utility of virtual servers that are controlled by an organization and accessible to end-users via the Internet. We define cloud computing as the provision of business applications that are accessible via the Internet using software and data stored on virtual servers. Cloud computing offers a commoditization of business technologies: infrastructure as a service, software as a service, and platform as a service, all online and in a Web 2.0 framework. When a third party controls any aspect of the "cloud," issues are created regarding data security, privacy and legal compliance. In a way, this has been the case ever since fixed data lines were replaced by communication solutions that bundled data from several companies. The third party tries to fully exploit the efficiencies of virtualization and commoditization of several traditionally proprietary functions (infrastructure, platform and software), but creates substantial legal risk at the same time.

The benefits of third party solutions to commercial applications are well established. From third-party software solution providers who leveraged the requirements of multiple customers, to outsourced infrastructure providers who invest in faster and better technology solutions than is possible for any single customer, third parties have always been able to use efficiencies of scale and commoditization to drive down the costs of providing a function. However, with these benefits come risks, some of which are highlighted below.

Data Storage and Transfer

In a conventional outsourcing arrangement, the customer can negotiate control over the location of its data,

including where backup operations will be conducted. This knowledge allows the customer and provider to know which regulatory schemes apply and to comply with the relevant data transfer laws. Outsourced cloud computing, however, can be delivered at a cost-effective price because the provider can move data around the world, perhaps splitting it up and sending it to different locations, depending on capacity, use and bandwidth. This freedom may result in non-compliance with the myriad worldwide regulations pertaining to storage and transfer of data.

Historically, the negotiation of risk between a provider and customer in an outsourcing arrangement usually relied on the customer requiring the provider to adopt certain processes that would result in data transfer regulatory compliance. Absent these requirements, providers were "not in the business" of concerning themselves with the specific legal data obligations applicable to the transfer and storage of the customer's data. But over time, providers have realized that to be responsive to customers, and still obtain economies of scale, they must integrate these requirements into their more generic solutions. Eventually, then, we believe cloud computing providers will internalize substantial parts of data transfer regulatory compliance into their commoditized offerings, accepting that the cost of compliance can be leveraged across a large-enough user community and built into the price.

For example, one early cloud provider allows the customer to have some control over where data is stored for selected services, through "availability zones." Because data transfer laws are country-specific, a cloud provider could store data in certain, pre-determined geographic regions (for example, the European Economic Area) and comply with the requisite transfer obligations for moving data out of the area. This way, data could be transferred endlessly within a cloud provider's European servers without running afoul of any data protection laws, because data is only stored only in a specifically requested region.

Data Security

Data security and data protection is always a major concern in any outsourcing arrangement. Outsourcing contract schedules specify exacting security management techniques that must be utilized by the provider. And, again, much of this is driven by data protection regulations for sensitive data, whether financial or personal. How can this be handled with a cloud computing solution? The CEO of Cisco has said that cloud computing "is a security nightmare and it can't be handled in traditional ways."[*] For most companies, data security and data protection are the biggest barriers to outsourcing cloud computing for any applications that involve sensitive or confidential data.

As with ASP, telecom transport, and Service Bureau agreements, cloud computing agreements will tend to be one-sided and not easily negotiated. For example, one cloud provider contract that is entered into online is non-negotiable and very provider-friendly: The provider makes no representations as to data security; places sole responsibility for security, protection and backup of data on the customer; and disclaims all liability for unauthorized access, use, corruption, deletion or loss of any data.

Therefore, contracts with cloud outsourcing providers will require more due diligence and involve less negotiation of terms and conditions. Customers should be concentrating on whether the cloud solution keeps them in regulatory compliance, and ultimately customers will rely on the provider's documentation of its solution as being compliant (either directly – as with a software release for banking or healthcare software - or indirectly, as in defining with specificity the locations where data will be stored). Consequently, a failure of the provider to keep the customer in compliance could be a failure of the service to comply with its own specifications, and result in a contractual damage remedy.

In due diligence, as in any outsourcing arrangement, reviewing the provider's solution to determine control of access to the data is crucial. Does the provider's solution allow you to limit access rights to your data, and monitor access so you know who accessed what and when? What are the specifications regarding encryption? How frequently is data archived, and are all applications and software kept current with the most recent security updates? Do service-level agreements include maintenance of security systems as a measured performance obligation?

Changing Providers

Another risk that must be considered in contracting for outsourced cloud computing services is to assure business continuity upon termination of the service. Most negotiated outsourcing agreements have negotiated exit plans and transition services, including delivery of data in a format that can be utilized with another provider or an in-house solution. A typical cloud service provider agreement would not address these concerns. For example, an online cloud provider contract allows the provider to terminate the agreement at any time and have no obligation to

maintain your data. At best, it promises not to *intentionally* erase any of your data for 30 days. This will not do. You must negotiate for termination services, including transition to another provider or in-house, and you should make sure data is routinely delivered to a back-up provider to ensure continuity of service in the event of a catastrophic failure.

Other Risks

Cloud computing solutions have many risks in common with other outsourced solutions, but these risks are harder to mitigate through negotiation. For example, outsourcing means transferring the measurement and reporting of service levels to the provider, relying on the provider's infrastructure to deliver key performance information. In a cloud solution, however, there is even less room for customization. Similarly, unless carefully negotiated, most outsourcing agreements yield inadequate compensation to the customer if things go wrong or the relationship doesn't work out; yet the cloud relationship tends to provide less room for negotiation of alternative remedies than a traditional outsourcing relationship does. Thus, where negotiated language is hard to achieve but the price of the cloud solution is too good to pass up, consider management of the risks through use of alternate providers, and similar techniques.

Suggestions

Because your company is liable for the way its data is handled, take steps to ensure that the cloud provider is complying with its obligations. Here are some data protection measures that are helpful when using cloud computing outsourcing:

1. Determine if cloud computing outsourcing is right for your application. If the function you seek to outsource involves sensitive information, it may not be the right choice. There will be transactions where cloud computing simply does not make sense until a robust offering that includes compliance is available.

2. Encrypt data before you send it to the cloud. Industry professionals agree that this is a good way to limit potential risk.

3. Control access to the data. Make sure that the provider has limited the people who can access your data, and ensure that access is properly monitored.

4. Keep in mind e-discovery obligations and the possible need to retrieve electronic records from the provider on relatively short notice.

5. Comply with all necessary regulations. Because your company bears the brunt of complying with data protection laws, make sure you know where data may be stored. The cloud provider must give you this information so you can assess the risk of non-compliance. If the provider does not share this information, then no sensitive information should be transmitted.

6. Control data location, if possible. This is the best way to ensure that the provider (and, by extension, the customer) is complying with data security laws. Limit the cloud to a definitive set of locations.

7. Make sure the provider is updating its protection systems, both as required by the contract and in accordance with industry best practices.

8. Ensure appropriate disaster recovery and business continuity plans are in place. Require the provider to archive your data so that it can be accessed if the system goes down.

9. Backup and/or store your data periodically with a party other than the cloud provider.

10. Use technology and compliance audits to be sure that data is secure and that systems are properly integrated.

11. Have clear procedures in place for the return of data in the event of termination or provider bankruptcy.

12. Actively monitor the relationship, and utilize service levels to ensure that the provider is complying with its obligations. Cloud computing outsourcing is no different from any other type of outsourcing in this regard: Success requires the customer to actively manage and oversee the relationship!

Footnotes

[*]R. McMillan, "Cisco CEO: Cloud Computing a 'Security Nightmare'," available at http://www.csoonline.com/article/490368/Cisco_CEO_Cloud_Computing_a_Security_Nightmare_