LTN Law Technology News

Negotiating Cloud Computing Agreements

Michael P. Bennett
03-11-2010

Cloud computing has been characterized as a paradigm-shifting phenomenon that will change how we purchase IT resources. Though given different names, cloud computing has been around for some time, and the legal lessons learned from experience with traditional software licensing and outsourcing agreements can and should be applied to cloud agreements, but there are new issues which will need new solutions.

Cloud computing is a loose term that describes a variety of data storage, processing, and application services, normally provided by a third party using equipment not located on the customer's site. These services include providing raw processing power on demand, special purpose applications on a subscription basis, and remote data storage. An early form of cloud computing was Application Service Provider or ASP services, and another is currently known as software as a service or SaaS. Cloud services are normally provided using internet technology, where the customer uses inexpensive hardware and an internet browser to access the service and/or remotely stored data.

The ease of access and simplicity of using cloud applications are part of its attraction. Unfortunately, the same cannot be said for the legal issues related to cloud computing. While traditional software licensing and IT outsourcing agreements can be used as a model for cloud computing, there are new risks and business practices not addressed in those older agreements that must be considered.

OUTSOURCING AGREEMENTS AS A MODEL FOR CLOUD AGREEMENTS

Cloud computing agreements are basically services agreements, as are outsourcing agreements. Many of the provisions included in outsourcing agreements have direct applicability in cloud service agreements. For example, the basic warranty that services will be performed in a good and workmanlike manner is a good starting point for warranty language.

Normally, outsourcing agreements will explicitly provide that a customer's data belongs to the customer, and that the vendor will give the customer a copy of its data at anytime. The customer is normally only charged for media and the vendor's time spent in providing those copies. Cloud agreements should contain similar provisions, but frequently don't. In fact, some agreements allow the vendor to hold the customer's data hostage if there is a dispute. Similarly, outsourcing agreements will frequently prohibit the vendor from suspending or terminating services abruptly. That prohibition prevents the vendor from exercising undue leverage in a dispute with the customer. Finally, outsourcing agreements normally require the vendor to provide termination assistance to the customer when the contract ends. This is normally provided at an hourly rate negotiated before services commence. Cloud customers will want to avoid agreements without similar protections, especially if the vendor is holding sensitive data or providing mission-critical services.

Similarly, outsourcing agreements frequently contain caps on fee increases. This prevents fees from rapidly escalating after a customer has made a long-term contractual or technological commitments to a vendor. Customers will want to include similar price protection clauses in their cloud agreements.

Outsourcing agreements also frequently contain a "litigation cooperation" clause which requires the vendor to preserve data and cooperate with discovery requests if the customer is involved in litigation. Those clauses allow the customer to fulfill its obligations in the event a litigation hold is required or it is served with discovery requests. The same issue arises under cloud agreements. If those cooperation clauses cannot be included in a cloud agreement, the customer should implement appropriate data backup plans to allow it to comply with its document preservation obligations in the event of litigation.

TRADITIONAL SOFTWARE LICENSES AS A MODEL FOR CLOUD AGREEMENTS

Cloud-computing agreements can also benefit from use of warranty terms found in traditional software licenses, where software is installed on a customer's own computers, usually on the customer's premises. For example, a traditional license

normally includes representations that the software will perform in accordance with written specifications. To ensure that customers obtain the desired functionality, cloud service agreements should contain a similar representation. Sometimes, cloud vendors incorporate these terms by reference, using documentation located on their websites. Those online documents, however, can be changed without notice and sometimes disappear completely. Other times, those documents are accessible only with a password, which is provided after the customer has signed up for the service.

As with traditional licenses, customers should insist on intellectual property ownership warranties or indemnity obligations to ensure that the vendor has the right to provide the service being provided and will protect the customer against claims that they don't.

NEW ISSUES UNIQUE TO CLOUD AGREEMENTS

Cloud agreements also raise new issues, which are not adequately addressed by traditional software or outsourcing agreements.

Inappropriate Terms Included in Cloud Agreements

Cloud-computing agreements utilize provisions found in agreements for other business models, including agreements for service, traditional licensing, and utility or pay-as-you-go models. The mixture of provisions from other models can lead to inappropriate terms being included in cloud agreements. For example, many cloud agreements aggressively disclaim warranties, or offer limited warranties that only extend for 90 days from commencement of services. In an agreement that can last many years, such short warranties are inappropriate and lawyers may wish to specify that performance warranties endure throughout the term of the agreement.

Similarly, traditional software license agreements normally disclaim any liability for loss of data. And cloud agreements frequently contain similar disclaimers. But in a cloud agreement, the vendor normally provides the hardware infrastructure, the operating system, the application, and the backup service. Under these circumstances, it does not make sense to absolve the vendor from all liability for data loss. Cloud agreements should specify backup schedules and customers should ensure that they are contractually comfortable with the vendor's backup policies and data recovery responsibilities. Customers should also be very familiar with the vendor's disaster recovery plan and make their own arrangements for backup and disaster recovery if the vendor's plans are inadequate.

Terms Left out of Cloud Agreements

Cloud agreements frequently fail to include terms from agreements for other business models that should be included, even when the legal issues presented by the two models are the same. For example, outsourcing vendors provide transition assistance to their customers. This assistance provides assurance to customers that they can transition their data and applications to another vendor if the agreement ends. Cloud agreements frequently don't address this issue, but should when the vendor is providing mission critical services or handling sensitive data.

Another issue frequently left unaddressed in cloud agreements relates to compliance with export and privacy laws. Export of some technical data is restricted by U.S. export laws. Similarly, most countries in Europe prohibit export of personal data to countries that don't offer protections equal to or greater than those in Europe. Those countries don't consider U.S. laws sufficiently protective, so absent compliance with special "safe harbor" rules, the export of data about European residents to the U.S. is prohibited. Under cloud agreements, the customer frequently does not know where processing takes place or where data is stored. Because of this, export, data flow, and privacy concerns are frequently overlooked.

ISSUES UNIQUE TO CLOUD COMPUTING BUSINESS MODELS

Many issues in cloud agreements arise due to its unique business model. Some of these issues can be addressed by adjusting terms found in agreements for other business models. Others will need altogether new solutions.

Leverage

Customers frequently purchase cloud services in incremental, as-needed volumes. Because of this, the amount spent at any one time is relatively small. By contrast, large, up-front expenditures characterize outsourcing and traditional software licensing transactions. Even though the total amount spent under a cloud agreement can eventually exceed the up-front expenditures made in outsourcing and traditional license transactions, the fact that the payments are spread out tends to diminish a customer's leverage. Added to that, many cloud vendors offer low-cost, but cost-effective solutions. This leaves them little room to offer robust warranties and remedies. This can result in cloud agreements containing terms unfavorable to customers. For example, in a cloud agreement, a vendor's maximum liability is frequently limited to fees paid in a one- or

two-month subscription period. Those fees are normally relatively small. But the maximum liability under a traditional software or outsourcing agreements can equal total fees paid under the agreement, typically much higher. Cloud customers may wish to negotiate maximum liability measured by aggregate fees paid or estimated to be paid over the life of the agreement.

Security Considerations

With traditional software it is clear that most, if not all, responsibility for security is with the customer. Similarly, it is well understood how to address security concerns in outsourcing transactions. Even though security may be qualitatively better in a data center, those improvements may not translate into enforceable provisions in a cloud agreement. The lack of customer leverage in cloud agreements, discussed above, may prevent customers from insisting on contractually favorable security provisions. Further, cloud vendors may be resistant to offering negotiated, one-off security terms because the equipment and resources used to provide their services are shared with many customers, making it difficult or impossible for them to customize their services to meet the unique needs of individual users. Also, security provisions are meaningless unless the customer can audit their efficacy. But allowing thousands of customers to individually audit the cloud vendor's security procedures would be extremely time-consuming. And allowing that many people access to a company's security procedure would itself become a security concern. Finally, cloud services are frequently offered through third-party providers that may have little ability or leverage to alter the security practices of the data centers from whom they are acquiring cloud resources, and are therefore unable to offer similar protections to their customers.

Flexibility

Some cloud vendors offer cookie-cutter solutions that can be very cost-effective if the customer's business problem is addressed by the standard offering. Because the offering is standardized, it may be difficult for the vendor to customize its application. Even when a vendor indicates that it can tailor its offering to meet a customer's requirements, those customers should perform due diligence to determine if the vendor has a proven track record of implementing customized solutions.

New Revenue Models

Unlike outsourcing agreements, cloud vendors frequently use a customer's data to gather analytics that are then resold or used for other purposes. In contrast, outsource vendors normally agree to use customer data solely in compliance with the customer's policies and solely for the purpose of providing services to the customer. If the company uses a cloud vendor, it will need to check that the cloud vendor's privacy policies match its own, or the company could be in violation of its own policy, or it may breach its contracts with its customers and violate federal and state laws and regulations.

Transition Concerns

Cloud computing applications are accessible through a browser. Normally, no special hardware, operating system, or application software is needed to access cloud applications. On the other hand, the cost of the back-end servers and software needed to run the cloud application could be very expensive. Or that software may be proprietary, and not commercially available for traditional licensing. To ensure ongoing access, especially for mission critical applications, customers should check with their vendor to ensure they understand what hardware, operating system, and other software is needed and how much it costs. And this information should be verified before a cloud agreement is signed so the customer can make appropriate transition plans.

Customers should also ensure that the software needed to run a cloud application is licensed under acceptable terms. Many cloud applications use open-source software, which can create problems for companies. Open-source licensing agreements often contain terms requiring users to freely publish and make available to others any changes made to the software code. Other agreements prohibit enforcement of patents against other users of the open source software. Some companies prefer not to use software licensed on those terms.

Cloud services agreements are more like service agreements than software licenses. This means that if a cloud vendor goes out of business, it is unlikely that federal bankruptcy law would protect a customer's ongoing right to access the applications provided by the bankrupt vendor. To protect against sudden loss of access, customer should ensure that their vendor is fiscally sound. Customers should also ensure that applications and other hardware and software are readily available from other third parties. And customers will want to ensure they have adequate data backup procedures in place and a copy of their data in the event the service becomes unavailable.

Complicated Contractual Relationships

Cloud services are frequently provided through resellers or application providers who in turn contract with data centers for the resources needed to run their cloud services. In those situations, because the customer does not have a contract

directly with the data center, it may not have any contractual remedy for failures in the data center. Customers should check if the application service providers own their own data center or if they rely on third parties for that service.

CONCLUSION

The rise of cloud computing has necessitated the development of new kinds of agreements to protect the legal rights of both vendors and users. While traditional outsourcing and software licensing agreements can be used as a model, the unique nature of cloud computing means contracts must address several new areas of legal liability and risk. As with any service agreement, it is incumbent upon all parties involved to ensure the language used adequately represents their interests and provides them with the protections they require.

Michael P. Bennett *is a partner in the intellectual property department at Wildman, Harrold, Allen & Dixon (Chicago).*