Bloomberg Law Reports® Technology Law

Strategies for Evaluating Cloud Computing Agreements

Contributed by Andrew Geyer and Melinda McLellan, Hunton & Williams LLP

A recent technical malfunction that knocked out websites and affected hundreds of businesses using Amazon's cloud computing services offered high-profile evidence of both the widespread popularity of cloud services and the potential consequences of storing company data in the cloud. The incident also drew attention to cloud service contracts, raising questions about performance levels and backups in the event of a service interruption. With more and more businesses seeking to take advantage of the efficiency and cost savings offered by cloud computing, the lessons of the Amazon outage underscore the complexities involved in negotiating cloud computing agreements.

In general, cloud computing agreements are served up as non-negotiable forms. Indeed, cloud providers may validly argue that tailoring their service agreements to individual customers negatively affects their ability to exploit the most valuable advantages of cloud computing. Cloud computing agreements often draw on traditional outsourcing or technology licensing models, but those types of agreements may not cover the particular risks associated with cloud computing. Below we discuss some of the key commercial issues and privacy and data security concerns to consider when evaluating a cloud services contract.

Service Levels. It has been widely reported that Amazon takes the position that its multi-day outage did not violate the applicable service level agreement. Most likely, that surprised a number of its customers. Given that cloud providers generally are not willing to change their service levels (which generally apply enterprise-wide across all clients), customers should be sure to understand the limitations and ramifications of a prospective cloud provider's guarantees, in particular: (1) how the cloud provider determines whether service levels are being achieved, (2) who is responsible for measurement, and (3) what exceptions apply to service level performance. Although cloud service agreements also commonly provide that service level credits are the customer's sole remedy for deficiencies, additional remedies may be appropriate if the failure has a material adverse effect on the customer.

Data Security Breach Notification. If a cloud provider suffers a security incident affecting customer data, the state and federal legal obligations to notify affected individuals apply to the customer as the owner of the data, not the cloud provider. The determination of whether a security event constitutes a legally reportable breach may be subjective in nature, and certain time limits may apply with respect to the customer's notification obligations. Because data security breach notification requirements generally are not included in cloud providers' form agreements, it may be necessary to add a provision to address how actual or suspected incidents will be reported to the customer. Such a provision would

serve to supplement and clarify the cloud provider's statutory obligations to report unauthorized disclosures of personal information to affected data owners. It is important that the agreement include a clear definition of what constitutes an actual or suspected security incident requiring customer notification, as well as the timing and other details regarding how the customer will be notified.

Legal Process Notification. Cloud service agreements often state that the cloud provider may disclose customer data maintained in the cloud for purposes of responding to a subpoena or other lawful request. If the customer wishes to respond or object to requests of this nature, the agreement should include an obligation on the part of the cloud provider to notify the customer of such requests prior to making a disclosure, unless the cloud provider is prohibited by law from doing so.

Use of Customer Data. Cloud service agreements typically set forth certain purposes for which the cloud provider may use customer data. For example, the cloud provider may state that it monitors or uses customer data "as necessary to operate this service or any other Provider service" or "to protect Provider's rights" or "in order to improve Provider's products." Customers should carefully review and evaluate whether they are comfortable with the uses contemplated by their prospective cloud provider's agreement, and consider whether to seek specific limitations on such uses.

Compliance with European Data Protection Law. Depending on a company's exposure to regulatory enforcement and other liability in the European Union, the EU data protection regime may create certain obstacles to the deployment of a cloud computing solution. Because EU law has specific restrictions regarding the processing and transfer of personal data, EU privacy counsel should be engaged to advise on the negotiation of cloud computing agreements if the personal data of EU residents will be involved. Customers should consider whether to contract for a representation that data originating in the European Union will not be transferred to jurisdictions other than those that are considered to provide adequate protection under EU law. Frequently this option is available only to customers that purchase premium or individualized cloud services.

Limits of Liability. In cloud service agreements, the cloud provider's liability often is limited to direct damages and is capped at an aggregate dollar amount for all claims under the agreement. Cloud providers commonly define the liability cap as a multiple of monthly charges, generally ranging from three to six months of fees. While this method of arriving at the limit is widely accepted, the actual dollar amount should be validated by each party in light of the potential damages. And, although these provisions tend not to be reciprocal, customers should consider whether their liability to the provider should be similarly limited.

Given that a customer's payments may be reduced by performance credits and other set-offs, if monthly charges are used to define the liability cap, the agreement should specify whether the cap is based on charges invoiced or scheduled to be invoiced, or on charges actually paid. Further, exceptions to the liability limitations should be reviewed for compatibility with the cloud services to be provided. For example, a breach of confidentiality or data protection obligations may result in damages that far exceed the liability cap and significant indirect damages, making an exception appropriate.

Indemnity. Indemnities may be of particular importance depending on the limitation of liability provisions in the agreement. Cloud service agreements often limit the provider's indemnification responsibility to third party claims for intellectual property infringement. In some cases, however, indemnification responsibilities may be extended to include other types of claims such as those arising out of or relating to (1) violations of law, (2) gross negligence, theft, fraud or other intentional misconduct, and (3) death,

personal injury and property damage (including data loss), and the cloud provider may request similar or reciprocal indemnities from customers. In addition, indemnification for costs associated with data security breach incidents involving customer information may be of particular importance in the cloud context. Note that the indemnities typically cover only third party claims; other contract claims are remedied through breach of contract actions.

Representations and Warranties. Cloud service agreements generally only warrant that the service will conform to the service levels, or that the service will perform in accordance with certain specifications. Depending on the type of cloud transaction involved, customers should consider including warranties covering issues such as additional standards of performance, compliance with law and the prevention and remediation of viruses. For example, customers whose services involve the handling, processing or storage of payment card information may need to ensure compliance with the Payment Card Industry Data Security Standard, and customers who are subject to the Gramm-Leach-Bliley Act or the Health Insurance Portability and Accountability Act need to consider their obligations to include certain safeguards for personal information in their service provider agreements.

Termination. A customer's right to terminate a cloud service agreement is typically limited to the provider's uncured, material breach. But since cloud providers frequently include contract provisions allowing them to change the features and functionality of their offerings at will, a customer may want to terminate the agreement due to service changes even if the contract has not been breached. Customers may be able to secure the right to terminate for convenience, but providers often require a reasonable notice period or payment of a termination charge in exchange for that flexibility. If the cloud provider retains the right to terminate the agreement other than in the case of a payment default, the customer may seek to secure termination assistance services to mitigate possible damage to its business caused by an unanticipated service interruption.

Note also that a data security breach incident affecting customer data in the cloud generally does not itself constitute a material breach of the agreement that would give rise to termination rights. Accordingly, the agreement should include a provision that expressly states whether a data security breach incident is to be considered a material breach of the cloud agreement.

Termination Assistance. Although termination assistance typically is not contemplated in a cloud provider's form agreement, under certain circumstances such assistance may be critical for the customer to ensure business continuity. A termination assistance provision would require the cloud provider to (1) continue performing its services for a specified period of time, and (2) assist with the orderly transition either back to the customer or to a new vendor. Even if termination is triggered by customer's non-payment, it may be possible to secure termination assistance from the cloud provider if the customer pays for such assistance in advance or establishes some other type of alternative payment arrangement. Such provisions also should specify the means by which the customer will retrieve data it has stored in the cloud, the timeframe for the retrieval or delivery, and format in which the data will be returned.

Secure Destruction of Customer Data at Termination. Cloud service agreements typically provide for the return or destruction of the customer's data upon expiration or termination of services, usually after a specified period of time and at the election of the customer. These provisions generally focus on practical concerns associated with recovering data to facilitate the transition to another cloud service, or on limiting the cloud provider's obligation to maintain data for the customer after termination. From an information security perspective, and to comply with certain data protection laws regarding the secure disposal of personal information, these terms also should

specify the secure disposal methods by which data will be destroyed.

In conclusion, although the quickening stampede to the cloud may be justified, the cloud services procurement process must include an informed analysis of the potential business, legal, financial and reputational risks involved. The list of provisions discussed above is by no means exhaustive, but it offers a starting point for evaluating cloud provider agreements.

Andrew Geyer and Melinda McLellan are senior associates in the Global Technology, Outsourcing and Privacy practice group at Hunton & Williams LLP. They can be reached at ageyer@hunton.com and mmclellan@hunton.com, respectively.