

5 Key Considerations When Litigating Cloud Computing Disputes

GERRY SILVER

Special to Law.com
January 13, 2012

Given the ever-increasing reliance on cloud computing, it is inevitable that disputes and litigation will increase between corporations and cloud service providers. The most obvious point of contention will occur if data in the cloud is lost, damaged, stolen or is otherwise rendered inaccessible for a period of time. In such circumstances, the corporation may be facing enormous liability and will seek to hold the cloud provider responsible, while the cloud provider will undoubtedly look to the parties' agreement and the underlying circumstances for defenses. This article discusses five key considerations for litigators representing corporations and/or cloud providers to focus upon in litigating cloud computing disputes.

BACKGROUND

Cloud computing is the process by which a corporation uses remote computing providers connected via the Internet, rather than internal servers and network drives, to store and access the corporation's electronically stored information. Cloud computing essentially consists of large blocks of server space that are owned and managed by cloud providers, which corporations essentially "rent" on an as-needed basis.

Renting cloud space has become increasingly popular in recent years because it saves corporations the cost of building and maintaining their own data centers, and allows them to ramp



Chadbourne & Parke's
Gerry Silver

up or down the amount of server space on an as-needed basis. For example, cloud computing allows retail companies to have access to more server space during the holiday season without paying for that space as it goes unused during the slower summer season. Cloud providers also provide software maintenance and updates, which allows corporations to reduce expenditures on software and information technology staff.

LITIGATION LIKELY TO INCREASE

When a corporation internally houses its own data and software, problems, of course, may arise. Data may be stolen, lost, damaged or rendered inaccessible, potentially causing the corporation to shut down all or parts of its business for a period of time, resulting in lost profits, lost customers and costs of remediation. However, since the corporation is in charge of its own data, it may have only itself to blame. On the other hand, when the corporation enlists a cloud provider and problems occur, the corporation has a clear target -- the so-called "expert" or cloud

provider. Thus, as more and more corporations rely on the cloud, litigation in this area is expected to increase.

For example, disputes arose in April 2011, when Amazon, a major cloud provider, experienced a severe cloud network crash that reportedly caused thousands of websites to shut down for days. Cloud customers complained of losses of valuable customer data and substantial business interruption.

LITIGATION CONSIDERATIONS IN CLOUD COMPUTING DISPUTES

When disputes or litigation arise in the cloud arena, there are five key items for counsel to consider, whether representing the corporation or cloud provider.

Limitation of Liability

In the event of a cloud disaster, the first place litigation counsel should turn, whether representing the corporation or cloud provider, is the limitation of liability clause generally found in the cloud services agreement. Corporations should check to see if they have a contractual means for recovering for losses from business interruption, including lost revenue, lost profits and lost goodwill. By the same token, cloud providers should consult the clause to determine the overall universe of potential liability, particularly whether the contract expressly disclaims any recovery for consequential damages, which would include damages involving third parties, (i.e., lost revenue, profits and/or goodwill). Another key is whether, in addition to a disclaimer of consequential damages, there is a cap on total damages. In cloud provider contracts, damages are often limited to fees paid

under the contract. The scope of the limitation of liability clause will be a major factor in determining which side has leverage in any dispute.

May the Limitation of Liability Clause Be Circumvented?

While clauses limiting liability to direct damages, disclaiming consequential damages, and/or capping liability at fees paid are generally enforceable, many states' laws provide that such clauses are not enforceable in the event of gross negligence or recklessness. While gross negligence is often difficult to prove, courts have been more amenable to a finding of gross negligence in instances of data loss, given the severe harm suffered as a result. For example, one court recently sustained a claim of gross negligence and/or recklessness in a cloud computing/loss of data case because it was alleged that the provider failed to take adequate steps to protect the data. *Clark Street Wine and Spirits v. Emporos Systems Corporation*, 754 F. Supp. 2d 474, 481-82 (E.D.N.Y. 2010) ("[i]n view of great damage to customers and business that breaches of a computer system may cause, a jury may find that the responsible entities, such as [the cloud provider], should take special precautions to protect these systems").

Thus, to attempt to circumvent the limitation of liability clause, corporations should search to see if precautions that perhaps should have been taken by the cloud provider were not. For example, were back-ups of data stored in different regions? Were banks of computers isolated from one another ready to take over if another zone failed? If data was stolen, what security measures were taken? If stolen by a rogue employee, what was the cloud provider's hiring process?

By the same token, counsel for cloud providers should endeavor to flesh out all steps taken by the cloud provider both before and after the issues arose to demonstrate that the cloud provider

acted reasonably, took numerous special precautions, and certainly did not act with gross negligence or recklessness.

Analyze Contract Claims

Even absent gross negligence or recklessness, the corporation may have several legal claims at its disposal, particularly breach of contract. Often cloud service agreements require the cloud provider to maintain certain service levels involving overall availability of data, numbers of critical or non-critical outages, and length of delays in responding to issues as they arise. Counsel for the corporation should determine if service levels were not met and if service level credits are due.

Further, there may have been breaches of several provisions of the cloud agreement, such as warranty provisions. Similarly, certain back-up steps may be contractually required and counsel should review the agreement carefully to discern each side's obligations in this regard.

On the flip side, the cloud provider should scour provisions regarding the corporation's obligations, and any contractual assumptions regarding the corporation. For example, problems in the cloud may have been caused by issues on the corporation's end, such as perhaps bad data imported from a company the corporation recently acquired, for which the corporation is contractually responsible.

It is of course imperative to analyze the root cause of the cloud issues and determine which side is at fault. Litigation counsel for corporations and cloud providers should line up the witnesses, emails and other documents necessary to prove their respective case.

Remedies

While having meritorious claims in a lawsuit may help the corporation down the road, when there are issues in the cloud the corporation may be in a crisis state requiring immediate action. Counsel for the corporation should consider whether it may be able

to obtain an injunction to require the cloud provider to take extraordinary steps to attempt to restore data. Both sides should consult the agreement to determine if the parties have agreed that a loss of or risk to data may constitute irreparable harm, entitling the corporation to an injunction.

Corporations may also wish to consider immediate termination of the agreement and a corresponding transfer to another cloud provider. However, many agreements may prohibit termination and transfer until services are paid for in full, which the corporation may be reluctant to do given the dispute. The cloud provider in any negotiation may use such a clause as leverage, while the corporation may need to seek a declaratory judgment allowing termination or an injunction requiring transfer without making any further payment.

Insurance And Indemnification

Counsel for each side should be sure to check applicable insurance policies for coverage, and timely place insurance companies on notice. Similarly, both sides should consider when any contractors or other third parties are at fault and seek indemnification relief accordingly.

Gerry Silver is a partner in the litigation practice at Chadbourne & Parke. He is reachable at 212-408-5260 or gsilver@chadbourne.com.