Legal Issues in Cloud computing – Part 2

by Nick O' Connell - N.oconnell@tamimi.com -

March 2013

Remote access computing services, whereby software applications, databases, data storage, network configuration and programming tools are made available to clients as a service, are becoming increasingly popular.

Cloud computing allows businesses to convert capital expenses associated with IT systems and infrastructure into operating expenses associated with platforms, capacity and applications. For many companies the business case is compelling. As with any business decision, it is important to be fully informed, and aware of the risks. In this article, the second in a series of two, we look at some further core legal considerations associated with cloud computing. (Part 1 may be found in the December/January edition of Law Update.)

Service levels and service level credits

As with most IT services agreements, service levels – which provide objective and measurable standards and help manage performance and quality – are also relevant to cloud services. One key difference, however, is that Cloud Service Providers will typically set service levels that are applicable to all their customers, and there will be little scope to negotiate. (The situation may be different if the cloud is a private cloud, or if the client is procuring a large volume of services.)

When negotiating service level credits, the CSP will typically seek to use their own servers as the point of measurement for service availability. In contrast, from the client's perspective, availability at the client's own computer is the natural point to assess availability. In practical terms, it is not always technically possible to use the client's computer as the point of measurement, although it may be possible to use the cloud termination point at the client's premises. If it can be justified by the business need, then a leased line connection to the CSP would provide a reliable connection, as well as scope for the client to argue that availability should be calculated on an end-to-end basis.

Another important point relates to the time period over which availability is calculated. For example, calculating availability on a 24/7 basis seems appealing, although if the real business need for the service is during business hours, then it would be prudent to calculate availability based on the hours of business. For example, 98% availability on a 24/7 basis over a period of a month would mean that up to 15 hours of down-time would be permitted; whereas the same level of availability calculated with reference to business hours on week days over the same period would mean only 4 hours of down-time would be permitted.

The use of service level credits as a means of addressing service failure is not uncommon. Clients should ensure, however, that sufficient details of the reasons for non-compliance with service levels is provided to them, and that recurring issues provide a basis for termination. Otherwise, there is a risk that the CSP will simply see service level credits as the 'price' of failing to provide a reliable service – and there will be little incentive for them to strive to meet the agreed service levels.

Some CSPs will try to include provisions whereby a service level bonus is paid if certain service levels are exceeded. Clients should consider the extent to which the marginal benefit of excess up-time over an already high up-time level is really a benefit worth paying for. For example, if the CSP offers 98% up-time as standard, is there really any value to the client in paying a bonus for 99% up-time?

Limits on liability

CSPs will typically try to limit liability. They may disclaim any warranties and describe their services as being offered ‘as is’, and they may seek to exclude direct, indirect and consequential damages. If they do not exclude direct damages entirely, they may seek to limit damages to a specific amount, such as the amount paid by the client for the services during a specific period of time.

When considering provisions relating to limitations of liability, it is important to review these in detail. The client should specifically consider whether the types of events giving rise to what the CSP has described as indirect damages are, in fact, indirect – or whether they are exactly the types of damages that are likely to arise if the CSP fails to adequately perform its obligations. (A good example is ‘loss of data’, and costs associated with manually inputting any lost data, both of which would seem to be obvious losses resulting from a failure on the part of a CSP.) Similar considerations arise in the context of force majeure provisions, which are typically used to provide for natural disaster type occurrences. Some CSPs may attempt to include events for which it is reasonable to expect them to bear the risk directly.

Seeking to agree an increased cap, or seeking to specify certain losses as direct losses is a reasonable approach for a client to take. Additionally, were a dispute to come before the courts in the UAE, there is some consolation in knowing that pursuant to Article 390 of the Civil Code, “The contracting parties may fix the amount of compensation in advance by making a provision therefore in the contract […], subject to the provisions of the law. The judge may, in all cases, upon the application of either party, vary such agreement so as to make the compensation equal to the harm, and any agreement to the contrary shall be void.” Additionally, Article 296 of the Civil Code provides, “Any condition purporting to provide exemption from responsibility for a harmful act shall be void.”

Lock-in and transition

The risk of technical or commercial lock-in needs to be considered at the outset. Technical lock-in refers to the risk that the manner in which the cloud services are provided means that it would be technically difficulty and/or costly for the client to migrate to an alternative provider. Commercial lock-in refers to contractual restrictions on the ability of the client to terminate; the absence of a right to terminate for convenience, for failure to comply with agreed service levels, or other reasons. When engaging a CSP, the client should ensure that the risk of lock-in is properly understood and addressed. Technology develops quickly, so the benefits of a long term engagement with a CSP may be short-lived, so the ability to move promptly to another service provider is valuable.

Business continuity is always a major consideration in the cloud, as failure of the services can significantly impact on business. Many clients seek to establish an exit strategy at the outset, and verify that the CSP is able to implement its part of the exit strategy, such as by locating, isolating and extracting the client’s data. The exit plan should specify the CSP’s responsibilities in the event that the client wishes to exit the CSP’s cloud, the format in which the client’s data needs to be delivered, and the timeframe in which the transition needs to be completed. It is also prudent to require the CSP to formally confirm that all the client’s data has been removed from the CSP’s system.

Al Tamimi & Company’s Technology, Media & Telecommunications team regularly advises on IT service agreements, including in a cloud context, as well as related issues such as data protection, document retention and confidentiality provisions. For further information, please contact Nick O’Connell n.oconnell@tamimi.com