

Between the Clouds: Best Practices for Selecting Hosted Solutions in the Transportation and Logistics Industry

MAY 8, 2017

Authors: [Jonathan R. Todd](#)

Transportation and logistics providers are increasingly adopting cloud technology to bring connectivity and scale to their core operating systems. This trend will continue for the foreseeable future. The [Cisco Global Cloud Index](#) projects that 92% of workload will be processed using cloud data centers by 2020. Cloud services offer many practical benefits to the lightning pace of today's global supply chains, however, they present a number of unique legal risks that may be unfamiliar. Fortunately, proper due diligence into vendors and knowledgeable negotiation of services contracts can help prevent the sunny skies of cloud computing from becoming thunderstorms.

The relative "newness" of cloud computing is appealing to industries that are time-sensitive, data-driven, and geographically expansive such as the transportation, logistics, warehousing, and distribution sectors. Cloud computing simply refers to accessing information that is stored elsewhere by means of the internet through a third party provider. Many vendors across a wide range of industries utilize the cloud to run applications and deliver services to customers in a few different ways. The largest and most common cloud service market is known as Software as a Service ("SaaS"). SaaS solutions are third party managed applications that are accessed by the customer via the internet. Any data entered into and stored by the cloud hosted solution will be physically stored on a third party's server even though it can be accessed anywhere. This certainly adds accessibility, along with a degree of disaster recovery and business continuity benefits, and yet it raises certain other areas of risk that are not associated with traditional software licenses.

Many do not realize that traditional hardware and up-stream service providers work behind the scenes, often hidden from view, to make the groundbreaking functionality cloud services work correctly. This maze of equipment, proprietary code, and providers, can take on characteristics similar to "double brokering" scenarios of which transportation and logistics professionals are all too familiar. It is critically important to understand what you are purchasing, and from whom you are purchasing, when placing your enterprise's entire operational capabilities online through a hosted TMS, WMS, or other core system.

Take time and conduct adequate due diligence when sourcing application and services vendors. In very simple terms, transportation and logistics companies should understand how data will flow through the system like freight through a supply chain. The following subjects are well worth discussion with your prospective vendors before you sign and write a check.

Key Questions to Ask Cloud Application and Services Vendors

- **Location** - Where is your data stored? In the cloud . . . right? No, it will be on a server that is physically located somewhere in the world. You need to find out where, including the specific facility address, how many other customers will have data on the same server, whether the data will be moved to other countries, and whether the location and equipment is owned or leased by the vendor? It is often the case that the vendor doesn't actually host your data, despite what you may believe, and instead uses a third-party data center. You don't want to find that your data was actually hosted overseas by disreputable providers where laws regarding privacy may vary and U.S. export controls may be triggered!
- **Prevention** - What data-security systems are in place? The vendor should have security policies that are industry standard and recognize certain regulations. You should also consider the vendor's disaster recovery plans and breach notification procedures. You don't want to find yourself in the headlines due to a data breach, without your operating system for an extended period of time, or liable for a breach of your customer contracts. The vendor should allow for audits and penetration testing of facilities and systems to confirm it's representations.
- **Protection** - Will the vendor or other customers access or use your data? Who will see your data? Will your sensitive data be encrypted? Should it be? Will your data be treated as confidential information? Does the vendor sell your data, in the aggregate or otherwise? Will the vendor claim ownership in your data? Will you receive the data following termination of your contract? How fast? Who pays for the transition services to move the data to another vendor? These are all questions you need to ask. You don't want to learn that the vendor or your competitors were using your data against your interest - and now claim that they own rights to it.
- **Uptime Guarantees** - Does the vendor guarantee that you will have access to your critical software solution without interruption? The vendor should have clear service-level agreements with uptime commitments, response and resolution times, and remedies in the form of termination rights and credits or refunds.

Once you have found a vendor with whom you are comfortable, it is important to carefully read and negotiate the contract for your license or subscription service. Most reputable vendors will entertain your requested changes and additions to contract language, and many will make those changes prior to signing. You may want to consider other vendors if they are unwilling to negotiate with you or provide credible answers that meet your needs. The terms you accept should both address and be consistent with your complete understanding of the Key Questions above, otherwise you could put your company at risk for service interruption, loss of data, and the resulting increase in cost and loss of business.

Additionally, make sure that the commercial terms (price, number of user seats, data volume) align with your expectations, that the functionality (connectivity, visibility, data analysis, reporting, internal and external interfaces) is completely spelled out and adequately meets your needs, and that there are no extra-contractual (such as online) terms and conditions incorporate by reference. The most important issues that arise in contract negotiations with cloud service vendors involve indemnification, limitations of liability, and warranties. Consult with an attorney familiar with your business and cloud solutions if you are ever in doubt of whether you are protected in your cloud provider relationships,

Jonathan Todd is Of Counsel with the national transportation and logistics practice group of Benesch, Friedlander, Coplan & Aronoff. He may be reached at 216-363-4658 or jtodd@beneschlaw.com. Justin Clark is an Associate with the firm's innovation, information technology, and intellectual property group. He may be reached at 216-363-4616 or jclark@beneschlaw.com.