VENABLE® LLP

Articles

March 28, 2012

Know the Risks Before You Head to the Cloud: A Primer on Cloud Computing Legal Risks and Issues for Nonprofits

AUTHORS

Armand J. (A.J.) Zottola

RELATED PRACTICES

Technology Transactions and Outsourcing

RELATED INDUSTRIES

Nonprofit Organizations and Associations

ARCHIVES

2012 2008 2004
2011 2007 2003
2010 2006 2002
2009 2005

Related Topic Area(s): Copyrights and Trademarks, Electronic Communications, Meeting, Vendor and Government Contracts, Miscellaneous

A "cloud" solution is generally typified by remote access to computing resources and software functionality and frequently involves the storage and maintenance of related data. Today, cloud computing facilitates applications, e-mail, peer-to-peer communication, content sharing, and electronic transactions or storage for nonprofits. In many respects, the “cloud” has become a synonym for the “Internet” as cloud computing now encompasses nearly all available computing services and resources.

Cloud offerings utlilized by nonprofits tend to come in three flavors. Infrastructure as a Service (IaaS) offerings deliver information technology infrastructure assets, such as additional computing power or storage. Platform as a Service (PaaS) offerings provide a computing platform with capabilities, such as database management, security, and workflow management, to enable end users to develop and execute their own applications. And, Software as a Service (SaaS) offerings provide software applications on a remotely accessible basis. SaaS offerings are probably the most commonly understood type of "cloud" solution.

Cloud computing solutions can avoid the traditional need to invest in computer hardware and software resources required for on-site computing power and related storage equipment and space. Costs therefore evolve from capital expenditures for information technology equipment and resources to operating expenses for the cloud providers’ fees. Cloud computing also can minimize the need for on-site, technical support service expertise that would traditionally be required to implement, maintain, and secure computer hardware and software resources. Consequently, cloud computing offers nonprofits software and storage capacity and capability without the need to invest in as much infrastructure, personnel, and software licensing.

These benefits create flexibility and potentially lower costs for the cloud customer. It is therefore not surprising that this type of computing solution has rapidly become a key component to the operation of many nonprofit organizations. Despite these potential benefits, cloud computing doesn't come without risk. Below is a list of legal risks and issues for a nonprofit to consider when procuring or using a cloud solution. These risks and issues can appear as either a contractual or an implementation issue.

Take It or Leave It. Many cloud solution agreements are non-negotiable or more favorable to the provider than the end user, which places a greater emphasis on pre-negotiation analysis in order to work around inflexible contracts.

All Services, All the Time. All computing and software providers are morphing into service providers, and this change may impact the fee structure, term length, and available warranties.

Law Is Behind the Times; Contracts Even More Important. Existing laws and governance models have not kept pace with technological development, and this may leave the contract as the only means for dispute resolution.

It's All Online. Privacy and information security concerns will only increase with cloud usage.

Less Control of Subcontractors. Cloud providers tend to use subcontractors for hosting, storage, and other related services, and these subcontractors may not be readily known or otherwise liable or responsible for performance under the agreement.

Some Things May Not Be Worth the Risk. The inherent risks associated with cloud computing may make its utilization inappropriate for mission-critical I.T. services or resources

Not Everybody is on the Same Page. Different cloud solutions on different hardware may increase the possibility of incompatibility with outside software or network systems, i.e., compatibility will be dictated by the provider and not by the customer.

Know Your SLAs. Service level agreements (SLAs) vary and may be inadequate and unchangeable.

General Outages May Be Likelier. Shared resources may increase susceptibility to a single-point of failure.

Only What You Need. The terms of a license agreement may not fit the service being offered, e.g., cloud providers may grant themselves a greater right to use a customer's data or materials than necessary to provide the cloud solution.

Own Your Data. It will be more imperative than ever to hold on to the ownership and secrecy of data and materials used with the cloud solution in order to retain rights and ensure confidential treatment.

Don't Allow a Vendor to Have Zero Responsibility. Be wary of excessive disclaimers and limits and seek the implementation of a credit or refund structure to address outages and downtime.

Am I Covered? Check available insurance policies and consider the insurance policy of the cloud provider to determine if it covers business interruption caused by vendor failure.

Know the Exits. Know how to terminate a relationship with a cloud provider and plan for how such termination will unfold in order to minimize disruption caused by transitioning to a new service provider.

Where's Your Data? Understand where a copy of all stored data is physically located.

Seek Jurisdictional Clarity. Data transfer is easy and can create jurisdictional issues because the sites where data is located or transferred and where the related services are performed or received can and will typically be different.

You Need Access to Your Data. Know how to access, audit, hold, and retrieve all data or understand the limits on such data access because regulations and e-discovery rules may mandate particular data storage, protection, and transfer protocols.

Don't Forget Compliance with Law. Regulatory compliance may extend to the cloud provider, particularly, for health, financial, educational, or children's data, and laws and regulations governing privacy and information security.

Rules Are Different Overseas. The United States has more permissive data and database rules than many other countries, particularly by comparison to Europe, where greater restrictions and rights exist.

Will It Still Be There When Disaster Strikes? Understand the cloud providers' business continuity and disaster recovery practices.

Incorporate Overall Risk Management Strategies. Cloud computing risks may expand the notion of risk from I.T. management to operational management or regulatory compliance.

Everybody Is a Renter. Limited-term software licenses will become the norm with customers not having any ownership rights in the software copy being licensed.

Courts, governmental authorities, and industry standard-setting bodies may address some of the foregoing concerns. But, until then, nonprofits considering cloud computing solutions will need to look to their written contracts as the primary vehicle to protect their rights and ensure performance. Moreover, careful due diligence of cloud providers becomes key. Nonprofits therefore should consider multiple providers and should not make decisions based purely on cost. Instead, nonprofits should seek references and involve their key decision-makers and outside advisors to assist with the procurement process in order to ensure a thorough evaluation of the potential risks and issues with cloud computing.

A.J. Zottola *is partner in Venable LLP's Technology Transactions & Outsourcing Practice, and he works regularly with the firm's nonprofit clients. For more information, contact Mr. Zottola at 202-344-8546 or* ***ajzottola@venable.com****.*