Understanding And Mitigating The Legal Risks of Cloud Computing

By Bennett B. Borden and Shannon Smith

It is no secret that an increasing number of enterprises are investing in cloud computing. Whether they are replacing on-premise applications or traditional outsourcing models, rising costs and technical complexity have led organizations to look to third-party providers for some or all of their information technology needs. There can be significant economic efficiencies realized by moving to the cloud. But, just as important are potential benefits associated with data privacy and security, compliance, business intelligence and overall information governance improvements. Entities often struggle with establishing comprehensive information governance programs that capitalize on the value of their information assets while avoiding the risks of ungoverned information. Cloud providers are increasingly aware of these challenges and are shaping cloud solutions to overcome them. That said, there are also potential risks involved if an entity does not adequately consider the information governance implications, especially those involving electronic discovery, when moving to the cloud.

Bennett B. Borden co-chairs the e-Discovery and Information Governance Section at Williams Mullen. A litigation attorney, Borden focuses his practice on Electronic Discovery and Information Law. He can be reached at bborden@williamsmullen.com. **Shannon Smith** is an attorney with extensive knowledge around records management, litigation readiness, and archiving solutions. She serves as an eDiscovery and archiving specialist for Commvault. Smith can be reached at ssmith@commvault.com.

Three Models

Cloud computing leverages economies of scale to reduce inefficiency and improve performance of IT operations. Essentially, there are three categories of cloud service models — Infrastructure, Platform, and Software-as-a-Service, commonly referred to as IaaS, PaaS, and SaaS, respectively. Infrastructure-as-a-Service involves outsourcing of equipment or hardware to support IT operations. IaaS providers include Amazon Web Services, Rackspace, and Nirvanix, among others. PaaS also includes outsourcing of hardware and includes providers like Microsoft Azure and Google Apps. The difference between infrastructure- and platform-as-a-service is typically around control. With IaaS, a client is usually responsible for the configuration and maintenance of operating systems, whereas with PaaS, the service provider manages those responsibilities. Last, there is Software-as-a-Service, which is a software distribution model where applications or programs are hosted by a third-party provider and are made available over a network, usually the Internet. SaaS providers include SalesForce.com and CaseCentral, among others.

Legal Issues

Most enterprises are finding that moving to the cloud may improve overall IT cost-effectiveness, but the shift raises a number of issues on the legal side of the house that often go unrecognized or unaddressed. Although much of the early discussion around cloud computing focused on availability and security, the conversation has now shifted to topics like custody and control, authenticity and legal preservation. The existence of vast amounts of electronically stored information (ESI) housed offsite, the potential lack of control of this data, and the challenges of preserving and processing it in connection with a lawsuit or regulatory investigation is enough to cause concern among even the most technically inclined corporate legal teams. However, when carefully considered, information governance policies and procedures can be developed to reduce the risks and realize the benefits of cloud computing.

Impact of Cloud Data on eDiscovery Process

Identification, Preservation, and Collection

When corporate data is managed by internal IT resources, the number of data repositories and the physical locations of that data are finite and more or less easy to pinpoint. The enterprise controls how this data is created, stored, distributed and disposed of, and policies and procedures can be developed to respond to litigation or regulatory investigations with some surety. Data stored in the cloud, however, could be stored on multiple servers across multiple jurisdictions, making it more difficult to identify, preserve, and collect for litigation or regulatory investigations.

To ensure that an enterprise can demonstrate to a court or regulator that it took reasonable steps to address relevant ESI, it is important that corporate counsel ask the right questions about where and how data is being stored by a potential cloud service provider before making the decision to move to the cloud. The answers to these questions should be documented so that when a lawsuit arises, corporate counsel and IT can work quickly to locate responsive ESI. To this end, it is also important to note which tools are available to support the identification process. For example, does the provider offer search tools or other capabilities that would allow inside counsel to locate a certain subset of data?

Just as any prudent organization would develop policies and processes to preserve onsite data, information stored by a third party should also be addressed by corporate information governance policies. Will the cloud provider execute a litigation hold or are there tools available that would allow corporate IT or legal to execute a hold against data in the cloud? If the cloud provider

continued on page 4

Cloud Computing

continued from page 3

will not implement the hold, it is critical to understand and document the process for preserving ESI prior to facing litigation. This includes understanding your cloud provider's retention and backup policies and how data can be retrieved before it is potentially destroyed.

Collection can often pose the trickiest challenges when dealing with data stored in the cloud. Corporate counsel will want to understand what the collection process truly entails. For example, are there tools available to cull down data prior to collection or must all data be collected and then processed internally? Secondly, does the provider allow for self-collection and, if not, are there costs associated with data retrieval? Finally, it is important to understand the format of the collected data and how, if at all, the authenticity of the data will be affected by the collections process. Will metadata be altered as a result or can the cloud provider demonstrate that the data has been maintained in its original, unaltered state?

The key point is to do sufficient due diligence on a potential cloud provider and the specific solution it proposes so that policies and procedures can be developed that are crafted to the specific solution.

Reducing Other Risks of Cloud Data

Knowing the answers to these questions before an enterprise is faced with litigation is critical in reducing risk associated with identification, preservation, and collection. However, the e-discovery process is only one piece of the puzzle in governing corporate data in the cloud. Prior to entering into an agreement with a cloud provider, IT and corporate counsel will also want to jointly address the following subjects:

Record Retention and Backup Policies

Part of the identification process involves understanding what data resides in a corporate environment at a given time, which is one of the reasons that organizations develop and regularly update corporate retention policies. Moving to the cloud will likely add to the complexity of adhering to these policies. Will your cloud provider have the ability to execute corporate retention policies? How will the data disposition process be carried out and will it be documented? These are questions to pose to your cloud provider and include in your service agreement to the extent possible. If they cannot be included, then the information governance policies and procedures of the entity should be crafted to work within the strengths and limitations of a particular cloud offering.

Type of Data Being Stored in the Cloud, and Physical Location

In reality, negotiating the terms of the cloud service agreement may prove challenging. Some cloud providers only offer standard contractual terms while others might be willing to negotiate particular terms. With this in mind, it is important to consider what type of corporate data is being stored in the cloud and whether that data can be appropriately secured and governed. For example, if a provider is unwilling to provide the required level of service around privacy, security and authenticity, it would be unwise to store anything but the least valuable corporate data with a third party. Additionally, understanding and documenting where the data will be physically located is equally important. Companies must ensure their data is governed in accordance with whatever laws pertain to the location where the data might be stored. Also, the nature of the data may trigger location-specific issues, especially if the organization is managing information of foreign nationals where issues of privacy laws and/or blocking statutes may arise. Many cloud providers are competent with foreign privacy restrictions, however, and offer Safe Harbor certification, or will agree to restrict the movement or storage of data through or within specific jurisdictions. In this way, cloud solutions can actually strengthen the information governance policies of an entity.

Authenticity and Chain of Custody

Authenticity issues apply to cloud-stored data at any given time during its lifecycle. In order to ensure that the integrity of corporate data is protected at all times, it is critical to understand how the data will be moved into the cloud (if not originally generated in the cloud), out of the cloud, and how it is stored during its life in the cloud. How will the cloud provider ensure that metadata and content remain unchanged and that the data has not been tampered with in the cloud? Equally important is access to logs and reports to verify the security and integrity of the data. Last, you will want to include provisions in the service contract to ensure that the provider will comply with requests for declarations or other testimony necessary to establish chain of custody. As with other aspects of cloud computing, understanding these issues and crafting information governance policies and litigation response protocols around the specific cloud solution is critical to the reasonableness and thus defensibility of those policies and protocols.

Exit Strategy

Often overlooked, an exit strategy should also be discussed prior to entering a cloud agreement. As technology develops, it is likely that corporate IT may want to move data from one cloud provider to another to service its needs. Whatever the driver, corporate counsel needs to understand the legal ramifications of migrating data. How will authenticity and chain of custody be maintained and documented? What is the time frame associated with the migration? This latter question is critical given that an enterprise likely faces at least one lawsuit at a given time. Will the corporate legal team be able to respond to discovery demands if IT is in the midst of a large-scale migration? Finally, any costs associated with an exit strategy should be included in the cloud service agreement.

Conclusion

Although the above discussion may suggest that cloud computing is too risky to undertake, many organizations will discover that the benefits significantly outweigh these risks and, more importantly, that these

continued on page 7