Applying E-Discovery Best Practices to Cloud Computing

January 31, 2012 by Christine Soares

What implications will cloud computing have for civil litigation? This was the question posed by David Campbell, chair of the Advisory Committee on Civil Rules and professor Richard Marcus, associate reporter of the Advisory Committee in a June 29, 2011, memorandum to the participants of a "mini-conference" of the discovery subcommittee of the Committee on Rules of Practice and Procedure of the Judicial Conference of the United States. The conference convened on Sept. 9 to discuss the possible amendment of the Federal Rules of Civil Procedure to better address issues regarding preservation and sanctions in e-discovery.

According to the minutes of the mini-conference, attendees agreed that advancements in technology since the Supreme Court approved the e-discovery amendments to the Federal Rules of Civil Procedure have led to new challenges in ediscovery and preservation. Included among those advancements is cloud computing. The conference addressed cloud computing, calling it, along with social media, a "second generation" issue. One attendee noted the move to cloud computing will likely make the preservation and collection process "more settled," and recognized that e-discovery vendors will eventually evolve to handle e-discovery in the cloud.

However, U.S. District Court Judge Shira A. Scheindlin of the Southern District of New York, known for her expertise in ediscovery, recently raised the issue of the discovery consequences of storing ESI in the cloud. As Scheindlin remarked, "everyone now is talking about cloud computing, but ... many people don't know exactly what cloud computing is."

So, how will companies storing information in the cloud fulfill their obligations under the Federal Rules of Civil Procedure? The answer is not as complicated as it seems, but as with any defensible e-discovery strategy, it requires an in-depth understanding of the cloud computing model.

What is cloud computing? Simply put, the cloud is storage of data over the Internet. The National Institute of Standards and Technology defines cloud computing as "a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction." Most people who own a personal computer use cloud computing. Google's Gmail is one example where users can access e-mail on their laptops, desktops and PDAs from anywhere in the world. The server and e-mail management software is all in the cloud and managed by Google, the cloud service provider.

From a business perspective, cloud computing creates a virtual environment where data and information technology resources are housed outside of a company's own data center and accessed over the Internet. Cloud computing vendors use a global network of locations to house servers and may move data from one server to another to optimize storage space. Remarkably, cloud computing is reported to be able to reduce a company's information technology floor space by 80 percent and save significant costs.

Despite the convenience and the costs saved by storing data in the cloud, the identification, preservation and collection of ESI stored in the cloud can be complicated. However, by applying traditional best practices in e-discovery to cloud computing, companies can minimize risks and avoid adverse consequences.

Preliminarily, even if a party's data is stored in the cloud, the question under the Federal Rules of Civil Procedure is whether the data is within the party's control. Rule 34(a) defines discoverable information as documents or ESI "in the responding party's possession, custody or control." The federal courts have consistently treated data in the hands of a third party to be within the party's possession, custody and control. Therefore, the burden will be on the party to identify, preserve and collect ESI stored in the cloud.

Understanding the client's data management systems is the first step to e-discovery and will always be a critical component of any defensible e-discovery strategy. Traditionally, counsel will consult with the client's IT personnel to understand the company's information technology systems. Counsel and the client can create a data map outlining what data is available within an organization and where ESI resides. A data map can be created at any time, even before the client is involved in litigation.

With cloud computing, where data is not located in-house, data mapping requires a different approach. Counsel should first identify the client's cloud service providers and understand where the client's data is physically located. Before litigation, counsel should fully understand the client's cloud service providers' document archival and retention capabilities. For example, some cloud

service providers may not automatically preserve metadata, causing spoliation and exposing the lawyer and the client to sanctions by the court. In addition, metadata in the cloud may be inseparable among clients of the cloud service provider. As a result, production of one company's metadata could possibly disclose the metadata of another client.

The next step in managing e-discovery is preservation. Under the Zubulake v. UBS Warburg cases, the duty to preserve data is triggered whenever a party reasonably anticipates litigation. Once the duty is triggered, counsel should immediately issue a litigation hold notice. When the client stores data in the cloud, the litigation hold notice should issue to all of the client's cloud service providers.

However, as with traditional e-discovery practice, simply issuing the litigation hold notice is not enough. Before a party anticipates litigation, counsel should carefully negotiate the terms and conditions of the service-level agreement with the cloud service provider, ensuring that the contract includes language regarding the preservation of data for purposes of ediscovery and the timeframe within which the preservation process can be implemented. The provider should have the ability to stop end users from deleting relevant data.

Such provisions and defined capabilities will help the client avoid adverse consequences, including a court holding that ESI stored in the cloud is within the control of the client, despite the client's inability to compel the cloud service provider to preserve it. The provider should also agree to execute data retention and preservation policies before and after the client anticipates litigation. The contract should set forth policies related to the preservation of data and metadata in the normal course of business.

Carefully negotiating the service-level agreement with the cloud service provider is also vital in collecting ESI stored in the cloud. Before a client anticipates litigation, counsel and the client should know its cloud service provider's capabilities regarding ESI retrieval and collection. For example, does the provider restrict access to the company's data, which might preclude self-collection and increase the costs of collecting ESI? At a minimum, service-level agreements should address how the client and the cloud service provider will cooperate in responding to e-discovery requests.

Case law regarding e-discovery in the cloud is almost non-existent. However, as companies continue to use this advanced technology, federal courts will likely address e-discovery issues in the cloud and analyze the adverse consequences of cloud computing. In the meantime, counsel can continue to apply the Zubulake reasonableness standard and traditional best practices to e-discovery in the cloud.