

E-Discovery: The Stormy Nature of the Cloud

Author: David Meadows

Publication: InsideCounsel

Date: January 5, 2012

Outsourcing to SaaS-based technology in the cloud typically begins with a directive in the IT department to cut software license fees, storage costs and management overhead, but rarely includes the input of legal or consideration of legal e-discovery. This is when the volume of data being stored in the cloud becomes an extreme burden. Downloading hundreds upon hundreds of gigabytes of data from remote servers can be very time consuming. Depending on the litigation, you may have to perform multiple collections to ensure a complete collection due to timing issues.

The ideal solution would be to place select data on hold and only collect the data being held. The next best solution would be to conservatively hold broader categories of data and only collect data imminently needed for e-discovery. However, placing a legal hold on data stored in the cloud is challenging as there are no turn-key solutions to implement and manage this process. Some providers are working on integrating these features into their hosted solutions for email, but the execution and management is extremely cumbersome and an all or nothing solution implemented on an entire mailbox. Additionally, collecting data from the cloud can present new technology challenges. The IT department that used to be able to run scripts or other backend processes to collect data may find no such options are available with data stored in the cloud. Many times this process is developed during the heat of litigation, which increases the likelihood of mistakes and potential sanctions or adverse inference instructions.

To address many of the issues discussed above, the legal department should open a line of communication with the IT department and ensure the following questions are addressed:

1. What level of control or access to the organization's data is allowed by the cloud services provider?
2. Does the service level agreement with the cloud services provider include language regarding extraction of data for e-discovery?
3. Does the cloud services provider have documentation on their data preservation and collection processes?
4. Has testing been performed on the collection process to validate the integrity of the data and timing?
5. Does the cloud services provider keep and track appropriate chain-of-custody?
6. Is there a defensible process for preserving and collecting data from the cloud services provider?
7. What is the process for collecting data when the volume is too great to download from the cloud?
8. For international organizations, can data be hosted in select global locations to ensure compliance with local, national and international data privacy laws?

A successful cloud strategy is one that takes into account the potential obstacles for preserving and collecting information for the purposes of e-discovery. Knowing where the service provider's provisions end and where your organization's start is vital to ensuring a comprehensive, efficient and effective ESI request response.