

Cloud Computing: eDiscovery Issues and Other Risk

By Wendy Butler Curtis, with Curtis Heckman and Aaron Thorp

Cloud computing is an information technology trend that is here to stay. According to a recent survey, in 2009 alone, there was a 320% increase in the number of corporations testing or considering implementing cloud computing.¹

In cloud computing, software, resources and other technology are shared over the Internet and available to computer users on demand.² A company using cloud computing no longer internally owns and manages its IT systems, but instead contracts with a third-party cloud provider for these services. In short, cloud computing is a form of outsourced IT services. Cloud popularity continues to increase because it has very few up-front costs, does not require purchase or maintenance of significant hardware, and can scale to the need of the company without purchasing new software or hiring new personnel.

However, because of security, privacy and eDiscovery issues, it is essential that IT departments collaborate with counsel when instituting cloud computing solutions. Litigators also must understand how their clients are using cloud computing to ensure they make informed eDiscovery decisions and manage costs appropriately.

Security and Privacy Considerations

Security and privacy continue to be the top concerns in adopting cloud computing. Security risks are often more pronounced on the cloud because the company turns over custody of their data to the provider. If the cloud vendor shuts down unexpectedly, the data may be locked-in, leaving the company without the ability to protect, access or move the data.

Contact a Team Member

Wendy Butler Curtis
eDiscovery Of Counsel
Washington, D.C.
(202) 339-8584
wcurtis@orrick.com

Siobhan Handley
Partner
New York
(212) 506-3757
shandley@orrick.com

Kenneth Herzinger
Partner
San Francisco
(415) 773-5409
kherzinger@orrick.com

For more information about Orrick's eDiscovery practice group, please visit us on the web.

Previous eDiscovery Alerts

Qualcomm Six Ultimately Avoid Sanctions but Case Remains a Cautionary Tale (May 12, 2010)

Recent S.D.N.Y. Decision Declares Failure to Issue a Litigation Hold Gross Negligence and Outlines Standards for Preservation and Collection (January 26, 2010)

New California Electronic Discovery Rules Differ From Federal Rules in Notable Ways (July 14, 2009)

¹ Avanade, *Global Study: Recession Has little Impact on Cloud Computing Adoption* (Oct. 21, 2009), http://www.avanade.com/_uploaded/pdf/pressrelease/uscloudreleasefinal450600.pdf.

² Wikipedia, http://en.wikipedia.org/wiki/Cloud_computing (last visited May 5, 2010); see also Peter Mell and Tim Grace, *NIST Definition of Cloud Computing* (2009), <http://csrc.nist.gov/groups/SNS/cloud-computing/cloud-def-v15.doc>.

Unless a corporation elects to purchase a private cloud,³ in cloud computing, everything is shared. Regardless of whether the company uses a Platform as a Service⁴ or a Software as a Service⁵ model, the platform or software is shared with the cloud provider. Moreover, in non-private clouds, not only is data shared with the cloud provider, it is also co-mingled with other cloud customers. Thus, in at least one case, an entire public cloud server was seized per a search warrant directed at one company. As a result, several other companies' data was also seized and not returned until the investigating agency determined how to segregate the data on the server.

Migration to the cloud can also create international conflict of law and privacy issues. Depending on where the cloud server is located, moving data to the cloud may result in the transfer of data to a new jurisdiction such as the European Union, China, or India triggering certain data privacy requirements,⁶ as well as other security and regulatory considerations.

eDiscovery Risks and Impact on Litigation

There are numerous ways eDiscovery is implicated when using the cloud. Ownership and control, cost, destruction of data, and jurisdictional issues must all be considered.

First, when data is outsourced to a third-party cloud vendor, the data is still legally in the company's custody, control or possession under Fed. R. Civ. P. 34. The cloud does not change the company's legal responsibility to preserve and ultimately collect the data.⁷

³ There are four primary cloud models:

- *Private cloud.* The cloud infrastructure is operated solely for an organization. It may be managed by the organization or a third party and may exist on premise or off premise.
- *Community cloud.* The cloud infrastructure is shared by several organizations and supports a specific community that has shared concerns (e.g., mission, security requirements, policy, and compliance considerations). It may be managed by the organizations or a third party and may exist on premise or off premise.
- *Public cloud.* The cloud infrastructure is made available to the general public or a large industry group and is owned by an organization selling cloud services.
- *Hybrid cloud.* The cloud infrastructure is a composition of two or more clouds (private, community, or public) that remain unique entities but are bound together by standardized or proprietary technology that enables data and application portability (e.g., cloud bursting for load-balancing between clouds). Peter Mell and Tim Grace, *NIST Definition of Cloud Computing* (2009), <http://csrc.nist.gov/groups/SNS/cloud-computing/cloud-def-v15.doc>.

⁴ Platform as a Service, or PaaS is “[t]he capability provided to the consumer... to deploy onto the cloud infrastructure consumer-created or acquired applications created using... tools supported by the provider. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly application hosting environment configurations.” *Id.*

⁵ The NIST defines Software as a Service, or SaaS, as “The capability provided to the consumer... to use the provider’s applications running on a cloud infrastructure. The applications are accessible from various client devices through a thin client interface such as a web browser (e.g. web-based e-mail). The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings.” *Id.*

⁶ For further discussion of data privacy considerations see THE SEDONA CONFERENCE® FRAMEWORK FOR ANALYSIS OF CROSS-BORDER DISCOVERY CONFLICTS: A PRACTICAL GUIDE TO NAVIGATING THE COMPETING CURRENTS OF INTERNATIONAL DATA PRIVACY & E-DISCOVERY (Aug. 2008), http://www.thesedonaconference.org/dltForm?did=WG6_Cross_Border.

⁷ THE SEDONA PRINCIPLES ADDRESSING ELECTRONIC DOCUMENT PRODUCTION 48 cmt. 8.d. (2nd ed. 2007), http://www.thesedonaconference.org/dltForm?did=TSC_PRINCP_2nd_ed_607.pdf (“Many organizations outsource all or part of their information technology systems, or share data with third parties for processing or for other business purposes. In contracting for such services, organizations should consider how they will comply with their obligations to preserve and collect electronic data for litigation.”).

Accordingly, the legal department will need to know when IT is outsourcing company data relevant to potential litigation, especially e-mail.

Second, the cloud vendor may have either enhanced or limited technical abilities that will directly impact cost of preservation and collection. Be aware of these factors for budgeting purposes. If e-mail is outsourced, courts may assume, rightfully in many cases, that the cloud provider can, at little or no cost, enhance searching capability.⁸ Understanding these capabilities is also important in meet and confer sessions and motions practice to ensure the accuracy of any cloud preservation or collection representations.

Third, because an opposing party may seek information directly from the cloud vendor, the owner of the data may not even be aware that the cloud vendor has turned data over to the requesting party, government agency or court. To compound this problem, a cloud provider could retain information for a duration that exceeds a company's document retention policy. Thus, companies should require their vendor to follow the company's document retention schedule and destroy out-dated e-mails and other electronically stored information according to the company's internal policies.

Fourth, using a cloud may increase litigation exposure by providing additional contacts for jurisdictional determinations.⁹ It is, therefore, important to select a vendor who stores data only in jurisdictions where the company is prepared to defend litigation. Cloud servers may be located in other states, federal circuits, or even another country.

Mitigating Risk

Each of these areas of potential risk can be mitigated by: (1) carefully selecting the cloud vendor; (2) closely reviewing the service agreement; (3) executing a coordinated eDiscovery plan; and (4) contemplating an exit strategy should problems arise.

(1) Selecting a Vendor and Ensuring Proper Security

- Select an appropriate cloud model based on the type of information that will be moved to the cloud. Common models include private, public and hybrid clouds.¹⁰
- Look for a cloud model that contains redundancy. Though data loss rarely happens in the cloud, it has occurred and could result in lost profits, intellectual property or a court finding of spoliation and then resulting sanctions.
- Thoroughly investigate not only the vendor's encryption and access security, but also the security of the physical location of the servers. Work with your IT department to ensure the vendor has the appropriate data center certifications.
- Choose a cloud provider that performs background checks on its employees and requires the employees to sign confidentiality agreements.
- Determine a vendor's viability by obtaining its cash position and financial stability under non-disclosure agreements and insurance. If a vendor goes bankrupt, the company risks being locked out of its data.
- Evaluate whether the vendor has personnel who could testify as a Fed. R. Civ. P. 30(b)(6) witness or sign a declaration about how the company's information is maintained and preserved.

⁸ In *Capitol Records, Inc. v. MP3tunes, LLC*, 2009 WL 2568431 (S.D.N.Y. Aug 13, 2009), the court upheld the plaintiff's argument that the e-mail files the defendant sought to search were not reasonably accessible. However, the court noted that the day will come when the burden argument, based on a large organization's lack of internal eDiscovery software, will not be well received.

⁹ In *Forward Food LLC v. Next Proteins Inc.*, 2008 WL 4602345 (Sup. Ct. N.Y. 2008), the court found personal jurisdiction existed where a company's only contacts in New York was a single visit, a few e-mails to New York, and a server located in the state containing the corporation's virtual data room.

¹⁰ See *supra* note iii.

- Recognize that as more information and software is outsourced, the company's IT department will get smaller. This means there will be fewer people who understand what information is available and where that data is stored. Consider creating and maintaining a data map of data in the cloud or otherwise outsourced.

(2) Entering into a Service Agreement

The service agreement should address:

- *Records management* – require the cloud vendor to follow the company's destruction and retention policies, including retention, rotation and destruction of backup tapes.
- *Accessibility* – include a timeliness provision stating how long the cloud vendor has to deliver the company's data.
- *Customer support* – include a service guarantee to ensure there is adequate support, particularly when executing preservation or collection obligations or data transfer.
- *Legal policies* – specify how the cloud vendor will respond to a subpoena requiring production of the company's data.
- *Liability* – look for and examine any limited liability provisions.
- *Confidentiality* – require a privacy provision that contractually obligates the cloud vendor to keep the company's data private. Outsourcing does not absolve the company of complying with privacy requirements under statutes such as Sarbanes-Oxley, Gramm-Leach-Bliley, HIPAA, and Payment Card Industry Data Security Standard.
- *Length of Agreement* – try not to commit to a multi-year contract and include a severability clause. If any vendor issues arise, the company's data may be locked.
- *Termination* – detail how and when data will be transferred if there is a breach or termination of the contract.

(3) Executing a Coordinated eDiscovery Plan

- Develop a comprehensive preservation plan, identifying key contacts at the vendor who will be responsible for receiving the preservation notice and fulfilling the vendor's obligations under the notice.
- When a duty to preserve triggers, send a preservation notice to the identified contacts at the cloud vendor.
- Determine in advance how the electronically stored information will be collected, the format it will be provided in, and the best format for production.
- To the extent practical, ensure naming conventions, folder structures and other organizational tools are used in the platform in the cloud to allow for surgical collection and avoid the need to collect by search terms or other forms that result in over collection of irrelevant information. Know the data destruction procedures and policies of the cloud provider. Data that is improperly destroyed may be located and accessed by an unauthorized user or otherwise result in a data breach.
- Collection times from a cloud vendor will often take longer than an in-house collection, so account for this in your discovery plan.

(4) Contemplate an Exit Strategy

- Software as a Service and Platform as a Service providers often use unique proprietary applications and interfaces for their databases. Reformatting the data to be accessible by another provider may be costly and complex. If the vendor uses such proprietary software, attempt to obtain the source code under a non-disclosure agreement to make unexpected transitioning easier.
- Find a back-up vendor that utilizes the same on-premise systems as your current cloud provider in case the need arises for a quick move.

About the Authors

Wendy Butler Curtis is chair of Orrick's eDiscovery practice group.

Curtis Heckman is an eDiscovery Career Associate in Orrick's Global Operations Center in Wheeling, WV.

Aaron Thorp, Litigation and eDiscovery Project Coordinator in Orrick's Washington, D.C. office, provides process and technology consulting to Orrick case teams and clients.