"Cloud Computing" in Discovery
How We Deal with Electronically Stored Information

by Charles B. Molster III and Elizabeth H. Erickson

"CLOUD COMPUTING" is an e-discovery buzzword. In all likelihood, you and your clients are already using it, whether you know it or not. Cloud computing, sometimes referred to as Software as a Service (SaaS) or Platforms as a Service (PaaS), allows a company to store its data and software platforms or services in a third-party-owned and maintained "cloud."

By providing access to tools and applications through cloud computing, users can share resources that are independent of the user's hardware or physical location. There are a number of advantages and disadvantages to cloud computing, but the implications for e-discovery and the handling of electronically stored information (ESI) are numerous and should be considered and discussed by law firms and their clients.

Types of Clouds

There are two main types of clouds. The first is created when a client moves its infrastructure off-site to be hosted and operated by a third-party service provider. The second exists when applications are accessed through the Internet instead of being locally hosted and run. In this second instance, all data is stored in a third-party cloud. Cloud users do not have to download applications and software to their computers or mobile devices. Instead, they access the necessary services and information via the Internet.

Google is a widely used example of Internet-accessed cloud computing service. Google users all over the world use the company's online productivity tools and applications, such as e-mail, word processing, and calendars. Through Google, all of these tools are accessed for free.

Cloud computing allows users to access their data and services from virtually any computer with an Internet connection. This access often reduces costs because it takes clients out of the business of hosting infrastructure and shifts that job to an expert with pooled resources and advanced hosting skills.

However, the security of data located in the cloud continues to be debated. Skeptics — who generally lack confidence in the security of the Internet, likely due to the prevalence of cyber identity theft — question the reliability of clouds and whether confidentiality can truly be maintained in a virtual world. Those security concerns, however, are quickly being overcome or pushed aside in favor of the obvious cost and ease-of-use benefits of cloud computing.

Implications for E-discovery

Even at their simplest, clouds expand physical and virtual locations where electronically stored information might be found. This expansion may present a significant challenge during discovery. Because data is being stored off-site by a third party, cloud computing raises a number of questions about how e-discovery and data management are implemented.

A key consideration is who owns, manages, and accesses the ESI that resides in the cloud and is hosted by a third party. Rule 34 of the Federal Rules of Civil Procedure allows a party to serve a request for the production of documents and ESI that are in the responding party's "possession, custody, or control." In order to determine one's duties under Rule 34, one must first determine who owns and controls the data in the cloud — your client or the third-party service provider. Not surprisingly, most courts are likely to find that data in the cloud is within your client's control, despite the involvement of a third-party provider.[1] Clear ownership boundaries should be placed in the service contract to govern the relationship between your client and the third-party vendor.

When contracting with a cloud vendor, it is critical to ensure that the terms of the contract make clear that your client owns its data in the cloud; your client has the authority to manage its data; your client has the ability to access its data at any time; and your client's data is protected from inappropriate disclosure. With these issues clearly resolved in the contract, you should be able to prevent a vendor from hindering your discovery efforts by refusing to allow the necessary access and processing of ESI in the cloud.

Once you have resolved the "possession, custody, or control" issue, you need to determine how to satisfy your discovery obligations regarding such data. Unfortunately, cloud computing technologies are far ahead of e-discovery software developers. Many e-discovery vendors offer cloud solutions for hosting and reviewing data. However, the industry has not yet developed tools for conducting e-discovery against the cloud, including tools to easily perform preservation, search, retrieval, culling, and early case assessment against cloud infrastructures. But as more clients use clouds in their daily business, thorough, defensible discovery in the cloud will be needed. Clients will demand solutions that efficiently and effectively preserve, gather, and process data for discovery purposes.

Ultimately, the buzz around cloud computing is expected to continue, as new platforms arise and clients' confidence and usage evolve. Information technology and legal industries will need to respond with solutions that meet clients' operational needs, while simultaneously addressing the increasing demands of e-discovery in the cloud.

Tech continued on page 60

Tech continued from page 59

Endnote:

1 Few courts have specifically commented on discovery obligations within the context of cloud computing. However, in situations in which possession and control were similarly split between a party to litigation and a third-party service provider, a number of courts have found that sufficient control existed to impose obligations on the litigating party. *See, e.g.*, *Flagg v. City of Detroit*, 252 F.R.D. 346 (E.D. Mich. 2008) (finding that defendant had sufficient control over text messages held by third-party service provider); *Tomlinson v. El Paso Corp.*, 245 F.R.D. 474 (D. Colo. 2007) (where third-party vendor had possession, custody and control of the electronic data, defendants could not delegate their statutory obligations to preserve and maintain data and avoid discovery); *In re NTL Inc. Sec. Litig.*, 244 F.R.D. 179 (S.D.N.Y. 2007) (finding that defendant had the practical ability to obtain any documents it needed from a third-party corporation); *Zynga Game Networ, Inc. v. McEachern*, No. 09-1557, 2009 WL 1138668 (N.D. Cal. Apr. 24, 2009) (where defendant was sanctioned and ordered to cause a computer rental vendor to relinquish control of previously rented servers).