Portfolio Media. Inc. | 860 Broadway, 6th Floor | New York, NY 10003 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

When Cloud Computing Meets E-Discovery Obligations

Law360, New York (September 14, 2010) -- Companies are increasingly putting documents, information, e-mails and data in the hands of third-party vendors and then accessing that information through the Internet. Accessing data, information and e-mail on the Internet through a third-party vendor is often termed "cloud computing." The third-party vendor is often called a "cloud vendor." Cloud computing represents a sea change in the way that electronic information is accessed by businesses.[1]

Merrill Lynch has predicted that the annual global market for cloud computing will surge to $95 billion by 2013.[2] The use of third-party vendors to handle a company's electronic information is becoming more prevalent because companies are able to save money by avoiding capital expenditures on hardware, software and services. For example, Japan's Panasonic Corporation spends several hundred million yen per year on its own information system and expects to cut that cost by 40 percent by utilizing Oracle's cloud computing service.[3]

A company's utilization of cloud vendors can create legal questions with respect to the company's electronic discovery obligations in litigation. By utilizing cloud vendors, the company may not be in possession of its own electronically stored information ("ESI"). Yet, the company may be required to preserve and produce ESI to another party in litigation. A company utilizing a cloud vendor should make every effort to avoid a situation in which it is charged with the ability to preserve and produce ESI, but lacks the authority — or at least the clear authority — to discharge its obligations.

Federal Rule of Civil Procedure 34 provides that discovery may be had of documents and things that are in the "possession, custody, or control" of a party. The term "document" as discussed in the Federal Rules of Civil Procedure and in this article includes ESI. The same

terminology is also common, if not pervasive, in state discovery rules.

Determining whether a company has "control" is fact-specific. A party to a lawsuit can be charged with control of a document, whether paper or ESI, even if the party does not have legal ownership or actual possession of the document or ESI. This was the conclusion of a federal judge in New York in In re NTL Securities Litigation.[4]

In that case, the class plaintiffs filed suit against NTL Inc., claiming federal securities law violations.[5] NTL then entered Chapter 11 bankruptcy, and two new companies emerged: NTL Europe Inc. and NTL Inc.[6] NTL's bankruptcy plan permitted the securities lawsuits to go forward against any individual defendants and NTL Europe as the successor to NTL.[7] While NTL had sent out "litigation hold" notices to its key players directing them to retain documents that may be relevant to the lawsuits, these notices were not implemented effectively.[8]

In response to plaintiff's motion for an adverse inference instruction, NTL Europe claimed that it could not be held responsible for the destruction of the materials because it did not have control over the documents relevant to the plaintiffs' discovery requests.[9] Any discoverable information was supposedly in the possession of the new NTL Inc.[10]

In analyzing whether NTL Europe had the obligation to respond to a Rule 34 request for production of documents, the judge found that "control" does not require a party to have legal ownership or actual physical possession of any documents.[11]

Instead, the court concluded that such materials are under a party's control when that party has "the right, authority, or practical ability to obtain the documents from a non-party to the action."[12] The judge ultimately concluded that NTL Europe had the legal right and practical ability to obtain documents and ESI from NTL because of a document sharing clause in a contract between the parties.[13]

Similar to the NTL case, a number of other courts have focused on whether a party has the practical ability to ensure the preservation of documents and ESI, irrespective of the company's legal authority to access them.

In Ice Corp. v. Hamilton Sundstrand Corp., a federal judge in Kansas found that the ability to obtain documents on request is not dependent on the retention of ownership.[14] Legal ownership was not determinative of whether the party had control.[15] In fact, the judge found that Rule 34 requires the production of documents beyond the actual possession of

the party "if the party has retained any right or ability to influence the person in whose possession the documents lie."[16]

In Goodman v. Praxair Services Inc., a federal judge in Maryland focused on both the legal and practical ability to access documents and ESI in analyzing the control element.[17] In that case, the judge found that the defendant company did not have control over documents prepared by a contractor who worked for the defendant because the defendant did not have sufficient legal authority or practical ability to ensure the preservation of documents prepared by the contractor.[18]

Thus, the concept of "control" articulated by courts is a highly fact-specific standard whose precise application to a specific set of facts may not be entirely predictable. Control may be found to exist even where a party does not have possession of the documents or even the legal right to possess the documents. In fact, control may be found to exist where there is simply an ability to influence the person who has the documents or ESI.

In the context of cloud computing where a company's electronic information, data and e-mails are held by third-party vendors and accessed through the Internet, control issues are even more potentially nebulous. The company contracting with a cloud vendor should therefore try to clarify the cloud vendor's obligations as much as possible.

A business dealing with cloud vendors should carefully define and document contractually its relationship with these vendors to avoid a situation in which the business may be legally charged with "control" over ESI even though the business lacks the authority to compel the taking of all necessary steps to preserve and produce ESI held by the vendor that the opposing party is entitled to in the litigation.

Where important evidence is held by a cloud vendor and deemed to be within the control of the company that is a party to litigation, the company may be held responsible for preserving and producing the information, even where the cloud vendor is uncooperative. The court reached such a conclusion in Tomlinson v. El Paso Corp.[19]

In that case, a federal judge in Colorado found that the defendant ERISA plan provider had control over electronic records held by a cloud vendor even though the cloud vendor ultimately refused to produce the documents and the defendant was unable to access the documents.[20] Despite the inability of the defendant to obtain the documents from the cloud vendor, the court found that the defendant had control over the data held by the

cloud vendor because the defendant could not "delegate" its statutorily imposed duty to ensure that employee benefits records are accessible.[21]

A company utilizing a cloud vendor to process e-mail, information and data should act proactively at the outset of the relationship to ensure clarity as to the company's and the vendor's obligations and rights in the event of litigation, governmental investigations and similar proceedings having significant potential legal consequences. A careful delineation of the relationship will help avoid the scenario in Tomlinson, where the defendant was found to have control but not the ability to access electronic data held by its third-party vendor.

The contractual relationship between a company and a cloud vendor can involve numerous, and often technical, provisions protecting the ability of the cloud vendor's client to ensure discharge of its legal obligations as to its ESI in the event of litigation or expected litigation. But, at a basic level, the contract between the client and the cloud vendor should describe the access rights of the client to the ESI, as well as its ability to reasonably direct acts of the cloud vendor to preserve the ESI.

As to the latter, the contract should further address the cloud vendor's routine ESI deletion practices and protocols, and the circumstances in which routine deletion will be suspended on direction of the client. Routine deletion of potentially relevant data by a cloud vendor should generally cease when litigation is filed or there is a reasonable expectation of litigation and the cloud vendor has been notified to cease such deletion by the client.

A client company may get little or no sympathy from a court when ESI relevant to litigation should have been protected from loss but was deleted by a cloud vendor as part of its routine business practices, even though its deletion was not specifically directed by the client. If the court finds that the client had "control" — meeting any of the definitions employed in the cases above, including having the contractual "ability to influence" the cloud vendor's handling of the ESI — the client may be exposed to sanctions.

A company should also consider placing an indemnification provision (including attorneys' fees) in its contract with the cloud vendor in the event it becomes necessary to sue or subpoena the cloud vendor to protect the client's right to preserve and access its ESI. Negotiating such provisions into a contract is more likely where the client has significant bargaining power.

In some situations, smaller companies may not have as much bargaining power with a

larger cloud vendor. In dealing with electronic discovery issues in such a situation, the client company should clearly document its efforts to obtain electronic data from the cloud vendor and itself issue a subpoena to the cloud vendor if necessary.

At a bare minimum, the client should find out whether the cloud vendor has policies and protocols that will impact or interfere with access to the company's ESI stored with that vendor and understand those policies before choosing to enter into the cloud computing contract.

For companies in which litigation is a relatively common fact of doing business or where litigation is at least a reasonable prospect, the willingness and ability of a cloud vendor to carry out the client's litigation responsibilities should be an important service point and a basis for choosing another vendor where that willingness and ability are doubtful.

It remains unclear at present to what degree, if any, a company will be protected from judicial sanctions if it has placed its ESI with a cloud vendor with little or no contractual assurances that the cloud vendor will (or will be able to) accommodate the company's legal obligations in the event of litigation and that ESI is lost or difficult to obtain.

Certainly, the most desirable basic protection is a specific contractual provision with the cloud vendor clearly giving the company a right of full access to its electronic data at all times, backed up by reasonable due diligence by the company as to the cloud vendor's technological ability to carry out that provision.

--By Robert W. Pass and Rebecca N. Shwayri, Carlton Fields

Robert Pass (rpass@carltonfields.com) is a shareholder in the Tallahassee office of Carlton Fields and chairman of the firm's electronic discovery task force. Rebecca Shwayri (rshwayri@carltonfields.com) is an associate in the Tampa office of Carlton Fields and a member of the firm's electronic discovery task force.

[1] Rachael King, How Cloud Computing is Changing the World, Bloomberg Businessweek, Aug. 4, 2008, www.businessweek.com/print/technology/content/aug2008/tc2008082_445669.htm

[2] Id.

[3] Panasonic Embraces Cloud Computing to Cut Costs, Reuters, May 11, 2010, www.reuters.com/article/idUSSGE64A0LR20100511.

[4] In re NTL Inc. Secs. Litigation, 244 F.R.D. 179 (S.D. N.Y. 2007).

[5] Id. at 181.

[6] Id.

[7] Id.

[8] Id.

[9] Id. at 194-95.

[10] Id. at 195.

[11] Id.

[12] Id.

[13] Id. at 195-96.

[14] Ice Corp. v. Hamilton Sundstrand Corp., 245 F.R.D. 513, 516-17 (D. Kan. 2007).

[15] Id. at 517.

[16] Id.

[17] Goodman v. Praxair Services Inc., 632 F.Supp.2d 494, 515 (D. Md. 2009).

[18] Id.

[19] 245 F.R.D. 474, 477 (D. Colo. 2007).

[20] Id. at 477.

[21] Id. at 477.