

Cloud Computing—Discovery Problems, Risk Management and Smart Planning

David Barnard and Thyannda Mack, Lathrop & Gage

Cloud computing is becoming increasingly popular among companies desiring to cut costs while maintaining strong technical capabilities. It allows a company to eliminate the cost of owning and maintaining its computer systems by outsourcing these functions to a third party vendor. The "cloud" concept has been in general use for many years, primarily through personal services, such as Yahoo! Mail, Gmail, social media sites, Flickr, YouTube, etc. The user can upload, manipulate and then download his or her data using remote servers at little or no cost. A plethora of third-party vendors are now offering this same service to companies, providing companies an entire IT infrastructure service that is remotely owned and operated, and accessed solely via the Internet.

The unique nature of cloud computing raises a host of legal issues. Where does the data reside? What law governs? Who has control? What happens if data is lost? What happens if the system is hacked and privacy is compromised? What happens if the service is interrupted? This article focuses on recent cases that provide some guide posts to the future of discovery in cloud computing and advice on avoiding critical problems. Moreover, the check list of best practices provided to address these issues also can assist good general business decision-making about whether and how to best use cloud computing.

"Control" Goes Well Beyond Actual Control in eDiscovery

Federal Rule of Civil Procedure 34 allows for discovery of documents and things in the possession, custody or control of a party. For discovery purposes, the courts have defined control to include actual possession, ownership, legal right, authority, or sufficient legal or practical ability to obtain documents. "The concept of 'control' has been construed broadly."¹ Control does not require legal ownership or actual physical possession.

When using cloud computing, the client relinquishes possession, a great deal of physical control, and in some cases legal ownership, of its electronically stored information systems to a third-party. It may be unclear how much control the client has over its documents without specific contractual provisions defining the relationship and level of control of the documents and data. When litigation arises, the client may be held to be in control of and responsible for preserving and producing information over which it has no actual possession, custody or control.

Courts have even sanctioned parties in situations where a third-party refuses to produce or improperly destroys documents. While not all of these cases involve vendor relationships, similar reasoning can be applied. The courts have been

© 2011 Bloomberg Finance L.P. All rights reserved. Originally published by Bloomberg Finance L.P. in the Vol. 3, No. 2 edition of the Bloomberg Law Reports—Technology Law. Reprinted with permission. Bloomberg Law Reports[®] is a registered trademark and service mark of Bloomberg Finance L.P.

The discussions set forth in this report are for informational purposes only. They do not take into account the qualifications, exceptions and other considerations that may be relevant to particular situations. These discussions should not be construed as legal advice, which has to be addressed to particular facts and circumstances involved in any given situation. Any tax information contained in this report is not intended to be used, and cannot be used, for purposes of avoiding penalties imposed under the United States Internal Revenue Code. The opinions expressed are those of the author. Bloomberg Finance L.P. and its affiliated entities do not take responsibility for the content contained in this report and do not make any representation or warranty as to its completeness or accuracy.

especially strict when the party has a statutory duty toward the information that cannot be delegated.

For example, in *In re NTL, Inc. Securities Litigation*, the court awarded plaintiffs an adverse spoliation sanction and attorneys' fees against NTL Europe, Inc. after a discovery dispute over documents and electronically stored information that it argued were out of its control.² After entering Chapter 11 bankruptcy, NTL, Inc. split into two companies, NTL, Inc. and NTL Europe, Inc.³ NTL Europe asserted that it was not responsible for the destruction of documents at NTL, Inc. after an ineffectively implemented litigation hold.⁴ The court rejected NTL Europe's claim that the requested documents were not in its control even though they were possessed and deleted by NTL, Inc.⁵ The court found that NTL Europe, Inc. had a legal right and the practical ability to obtain the requested documents and electronically stored information due to a document sharing clause in a contract between NTL, Inc. and NTL Europe, Inc.⁶

In *Tomlinson v. El Paso Corp.*, the court granted the plaintiffs' motion to compel documents in the possession, custody, and control of a third-party record keeper, Mercer.⁷ It was undisputed that Mercer had custody of the documents; however, Mercer claimed trade secret status and refused to produce them.⁸ The court found that El Paso Corp's statutory duty under ERISA to establish a recordkeeping system and make the records accessible could not be delegated to a third-party.⁹ El Paso Corp. was therefore deemed to be in control and ordered to produce the documents.¹⁰

In *Flagg v. City of Detroit*, the court refused to preclude discovery into electronically stored communication maintained by a third-party service provider.¹¹ The Court found that the city had control over the text messages at issue noting several indicia of control.¹² As a subscriber, it has the power to block or permit disclosure by withholding or giving consent.¹³ The city as a public body also has a duty to furnish public records, which includes communications between public officials, for

inspection and examination.¹⁴ And finally, the court noted that the service provider could certainly provide a contractual mechanism for the city to access its own archived communications.¹⁵ Accordingly, the court found sufficient indicia of control to determine that the defendant's subject text communications were subject to discovery.¹⁶

In *Ice Corp. v. Hamilton Sundstrand Corp.*, the court granted the plaintiff's motion to compel Hamilton Sundstrand Corp. (Hamilton) to produce design documents in the possession of a third-party.¹⁷ The court found that a disputed contractual provision simply limited the form of access Hamilton had to documents, but did not change its ownership or control rights.¹⁸

Best Practices for Avoiding Cloud Computing eDiscovery Challenges

There are several ways that clients can protect themselves to help avoid these types of eDiscovery challenges. First, clients should be particularly deliberate when choosing a cloud computing vendor. Make sure the vendor is reputable, has the capability to do the job and a solid contingency/disaster recovery plan to ensure systems and data can be adequately protected. Second, carefully craft the service agreement, making sure to define the relationship to the information and between the company and the vendor. Finally, plan ahead for the prospects of litigation or a need to quickly transition between vendors.

When selecting a cloud computing vendor, it is important that clients:

- choose a cloud computing model that is appropriate for the information to be in the cloud,
 - For example, some models allow the information to be accessed by the public while others limit access to one or a group of particular organizations. Some cloud models only allow the

organization to access its information, while others allow an organization to actively manage the cloud infrastructure.

- ensure that the vendor has the appropriate capabilities, access, tools, resources, backups, security, and management,
- consider the availability and price of alternatives,
- understand the technical capabilities of the vendor, including its ability to assist in any investigation or production of documents that may be necessary,
- ask about the vendor's experience with eDiscovery response,
- understand what information is available, where it is stored (technologically and geographically), and how it can be accessed,
- select a vendor whose policies and procedures for retention, security, and confidentiality are similar to those of the client or require the vendor to adopt those policies of the client,
- investigate the vendor's financial viability, including insurance and non-disclosure agreements, to assess the risk of experiencing problems accessing data in the case of a vendor going out of business, and
- determine whether the vendor has employees who could testify as an expert witness or sign a declaration explaining the vendor's process for maintaining and preserving the client's information.

The next step is to clearly define client rights to data ownership and access in the service agreement. The parties should be sure to:

- define the relationship between the parties,

E.g. The parties are independent contractors. This agreement does not create a partnership, franchise, joint venture, agency, fiduciary or employment relationship between the parties.

- define policies regarding client access to the information, ownership, privacy, permitted and restricted uses, security, confidentiality, due diligence, retention, destruction, and the ability of the client to direct preservation or destruction of information, including creation, retention and destruction of backup resources,

E.g. As between the parties, the Disclosing Party exclusively owns all rights, title and interest in and to all of the disclosed data.

E.g. Except as otherwise permitted in writing by the Disclosing Party, the Receiving Party shall limit the access to Disclosing Party's confidential information to its employees, contractors, and agents necessary on a strictly "need to know" basis.

E.g. The Receiving Party shall maintain the appropriate administrative, physical, and technical safeguards for protection of the security, confidentiality and integrity of the Disclosing Party's data.

- mandate under what circumstances, in what time, and in what manner the vendor must supply the client's information or notify the client when providing information to the government, law enforcement, or any other requesting party,

E.g. The Receiving Party shall not modify the Disclosing Party's data, disclose the Disclosing Party's data except as compelled by law or expressly permitted in writing by

the Disclosing Party, or access the Disclosing Party's data except to provide the services contracted for or prevent or address service or technical problems, or at the Disclosing Party's request.

E.g. Disclosing Party is responsible for responding to third-party legal requests to disclose Disclosing Party's information. The Receiving Party will, unless prohibited by law or by the terms of the third-party request: promptly notify the Disclosing Party of its receipt of third-party requests in a manner permitted by law, comply with the Disclosing Party's reasonable requests regarding its efforts to oppose a third-party request, and provide Disclosing Party with information or tools required for Disclosing Party to respond to third-party request.

- require that the vendor provide adequate customer support and procedures for notification in the case of a security breach and include a provision directing how the vendor should respond upon notification of initiation of litigation involving the data or receipt of a subpoena regarding the information,

E.g. The Receiving Party shall provide basic support for purchased services at no additional cost, provide purchased services in accordance with applicable laws and government regulations, and make the purchased services available 24 hours a day, 7 days a week except for: planned downtime for which at least eight (8) hours notice will be given, or circumstances beyond the Receiving Party's control, including but not limited to acts of God, acts of government, flood, fire, earthquakes, civil unrest, acts of terror, or Internet service provider failures or delays.

- highlight any limited liability provisions, and consider including an indemnity provision that includes attorney's fees in the event it becomes necessary to sue to protect the right to preserve or access the information and a penalty for noncompliance that is significant enough to encourage compliance,

E.g. Receiving Party will indemnify, defend, and hold harmless Disclosing Party from and against all liabilities, damages, and costs (including settlement costs and reasonable attorney's fees) arising out of a third-party claim that the Receiving Party's technology used to provide the services caused any type of actionable claim.

- include a provision detailing the treatment and transfer of data upon termination of the agreement, and

E.g. Upon request by Disclosing Party made within 30 days of termination of agreement, Receiving Party will make available to Disclosing Party for downloading a file of Disclosing Party's data in comma separated value (.csv) format along with attachments in their native format. After a 30-day period, Receiving Party has no obligation to maintain or provide any of Disclosing Party's data and shall thereafter, unless legally prohibited, delete all of Disclosing Party's data in Receiving Party's systems or otherwise in Receiving Party's possession or under Receiving Party's control.

Finally, the company should plan ahead for possible litigation and termination of the cloud computing agreement. To do this the client should:

- create a complete preservation plan;
- identify the people who would play a critical role in fulfilling the vendor's role, receiving notice by the company, implementing the discovery process,

and providing testimony regarding policies and processes;

- determine a process and timeline for collecting, formatting, and providing electronically stored information for production;
- keep a backup vendor in mind, in case the need to transition quickly arises; and
- request source code if vendors use proprietary software, in order to anticipate the possible need for an unexpected or rapid transition. As a fall back, request a source code escrow agreement in the event vendor ceases to do business or support the necessary services.

Mr. Barnard and Ms. Mack are attorneys in Lathrop & Gage, LLP's intellectual property division. Their litigation work includes patent, trademark, copyright, trade secret and other commercial disputes in different courts throughout the nation. Their business counseling practices include assisting a wide range of companies in addressing intellectual property strategy, acquisition and risk management. They can be reached at dbarnard@lathropgage.com and tmack@lathropgage.com.

- ¹² *Id.* at 354.
- ¹³ *Id.* at 355.
- ¹⁴ *Id.*
- ¹⁵ *Id.* at 357.
- ¹⁶ *Id.*
- ¹⁷ 245 F.R.D. 513, 518-519 (D. Kan. 2007).
- ¹⁸ *Id.* at 519-520.

¹ *In re NTL, Inc. Securities Litigation*, 244 F.R.D. 179, 195 (S.D.N.Y. 2007). (citing *In re Flag Telecom Holdings, Ltd. Sec. Litig.*, 236 F.R.D. 177, 180 (S.D.N.Y.2006); *Dietrich v. Bauer*, 95Cv-07051at *3 (S.D.N.Y. Aug.16, 2000), *aff'd on reconsideration*, 198 F.R.D. 397 (S.D.N.Y. 2001); *M.L.C., Inc. v. North American Philips Corp.*, 109 F.R.D. 134, 136 (S.D.N.Y.1986)).

² 244 F.R.D. at 180-181.

³ *Id.* at 181.

⁴ *Id.* at 194-195.

⁵ *Id.*

⁶ *Id.* at 195-196.

⁷ 245 F.R.D. 474, 477 (D. Colo. 2007).

⁸ *Id.* at 476.

⁹ *Id.* at 477.

¹⁰ *Id.*

¹¹ 252 F.R.D. 346, 347 (E.D. Mich. 2008).