An ALM Website

January 17, 2012

CORPORATE COUNSEL

From the Experts: Don't Get Caught With Your Head in the Clouds

Ben Barnett and Regan Hunt Crotty

Among the most notable tech developments over the past year was the significant move by leading technologies companies such as Apple, Amazon, Google, and Microsoft toward cloud computing for both personal and business data. Indeed, a recent survey by Forrester Research Inc. found that 28 percent of all online U.S. adults use a personal cloud service, and 41 percent of them use cloud computing at work. This relatively nascent technology platform, however, entails some potential risks, particularly in the already complex area of e-discovery.

Regardless of whether your company currently relies on a cloud platform or is contemplating such a move, you need to honestly assess whether your company is currently in a position to identify, locate, preserve, and produce cloud data potentially responsive to litigation or an investigation. These questions need to be considered and worked through prior to litigation.

While the variety of internal IT and cloud structures makes prescribing specific solutions difficult, any prudent plan for managing e-discovery for cloud data should touch on the following areas:

Ben Barnett

Regan Hunt Crotty

Control

Federal Rule of Civil Procedure 34 requires that parties produce or make available "documents or electronically stored information" in the party's "possession, custody, or control." A handful of courts have already held that data stored in a cloud is indeed within a party's control, for purposes of Rule 34. See, e.g., *Columbia Pictures, Inc. v. Bunnell*, 245 F.R.D. 443, 453 (C.D. Cal. 2007); *Tomlinson v. El Paso Corp.*, 245 F.R.D. 474, 477 (D. Colo. 2007). Other courts may take this approach, given the increasingly widespread adoption of the "practical ability" test, under which the court considers whether a party has the practical ability to access the requested information.

As such, you should assume that your utilization of cloud computing does not absolve you of your discovery obligations, and you should establish at the outset of any relationship with a cloud computing vendor that your company controls the data stored in the cloud.

Jurisdiction

A central tenet of cloud computing is that your company's data is not stored on-site. While your business may be located in Philadelphia, your data may be stored in California or India. Thus, the question arises: Which law(s) govern the use of such data?

In order to avoid unforeseen and potentially costly legal exposure down the road, find out precisely where your data is being routed and stored and consider the jurisdictional implications. For example, does the storage of your data in another state establish the minimum contacts necessary to establish jurisdiction in that state? Or, if your data is being routed through another state or a foreign country, are you abiding by the myriad of potentially applicable laws, such as the Electronic Communications Privacy Act, the Patriot Act, the Health Insurance Portability and Accountability Act, the Health Information Technology for Economic and Clinical Health, the Gramm-Leach-Bliley Act, the Computer Fraud and Abuse Act, the FTC Act, and the European Union Data Protection Directive?

To the extent possible, address jurisdiction in your service provider agreement. In particular, consider mandating that your company's data be routed through and stored only in the United States, and require notification from the cloud provider of changes to data routing and storage jurisdictions. Given that cloud computing is still an emerging technology, be aware that there may be future litigation that could impact even the most carefully crafted jurisdictional provisions.

Record Retention

Your company's record retention policy may require that email be maintained for only two years. Your cloud computing vendor, however, may destroy email after six months, leaving you with lost data and facing potential allegations of spoliation. At the other end of the spectrum, your vendor may maintain data perpetually, leaving your company to sift through and

potentially have to review and produce years of documents that, per the terms of your own record management policy, should have been destroyed.

To avoid these inconsistencies, you need to align your hosting agreement with your company's record retention policy. This is particularly true for financial and tax records that are the subject of regulatory retention requirements. Specifically, you should consider establishing in your hosting agreement that data maintained on the cloud be retained just as it would be if the data was stored on your company's own computers. You may also consider adding a clause in your internal record retention policy to the same effect.

Preservation and Production of Documents

Given that in the cloud computing world you no longer have your data physically on-site, you may need to reassess your company's discovery SOPs. In fact, it would be prudent to consider developing a targeted discovery plan for cloud data. Such a plan, elements of which can be addressed in your service agreement, should:

- Identify a single contact person at the vendor responsible for overseeing data preservation and data production. You may also consider automating cloud-based litigation hold management.
- Describe the responsibilities of each party in implementing the litigation hold and providing documents and data.
- Identify in detail any additional costs charged by the vendor for document preservation and production.
- Confirm that the cloud provider can prevent cloud users from intentionally or inadvertently deleting or altering data that is subject to the litigation hold and can implement a targeted hold on just that data that is relevant to the litigation, rather than impacting (and potentially making inaccessible or slowing down) access to your company's data.
- Identify in advance (and potentially segregate) any personally identifiable data in the cloud that may be subject to either U.S. or E.U. privacy laws or directives.
- Set forth how the data will be collected, in what format, the time frame, and how it will be organized (e.g., naming conventions, folders, etc.).
- Identify who will certify any document or data searches and productions. Your company's employees may not be familiar enough with the vendor's technology to certify a search.
- Identify what happens if the relationship between your company and the cloud provider ends, particularly in the middle of litigation. Your company must be able to obtain its data, regardless of your vendor's business circumstances. Even if the vendor agrees to give you access to your data, be certain that the data is available in a usable format, and is not maintained in a proprietary or incompatible system. In some instances, it may be necessary to reserve the right to seek source code from the vendor. In addition, consider having a backup cloud provider available for the migration of your cloud data.
- Consider making explicit that the vendor is not an agent of your business, in an effort to shield your company from liability in the event that the vendor fails to properly preserve your data. Be aware, however, that some courts take a hard line on document preservation.

Even if your service agreement addresses all of these issues, you should continue to document your efforts to preserve and produce data and identify the steps you have taken to safeguard the data. This record may prove critical down the road in demonstrating good faith in the face of a spoliation allegation.

Other Important E-discovery Issues

There are several other potential e-discovery issues that you should consider in negotiating your service or side agreements, including:

- Indemnification of losses resulting from any security breach. Try to avoid limitations on liability, or at least negotiate a high cap.
- Requiring the vendor to sign a confidentiality agreement to protect your confidential data. Several states have considered the ethical issues faced by lawyers regarding the storage of confidential client information on clouds, and while law firms face unique concerns related to the storage of client data on clouds, more broadly it is advisable to review state privacy laws for states in which your company does business.
- Whether the storage of privileged data on a cloud constitutes a privilege waiver is an open issue. You should try to take the following steps to try to maintain the attorney-client privilege: (1) include a "no-waiver" provision; and (2) include a provision in which the vendor affirms that it is merely storing data and disclaims the right to read, review, disclose, transfer, or in any way use information stored by your company on the cloud.
- Maintenance of insurance by the vendor.
- Compliance by the provider of all laws pertaining to its business and performance of the services contemplated by the agreement.
- Trying to avoid multi-year contracts that tie you to a provider, particularly one without an extensive track record.
- Implementing a Severability Clause.
- Segregation of your company's data from that of other businesses.
- How the provider will respond to a subpoena for your company's data or another company's data. Data is often shared on a cloud, and you do not want your data to be produced simply because it is stored in the same cloud as a subpoenaed company's data. Moreover, you should have a notification process in place where, consistent with current law, you are provided notice of any subpoena concerning your company's data.
- Whether the provider subcontracts the data storage and how that affects your agreement.

The advent of cloud computing offers companies significant business and IT benefits. In order to achieve these benefits and appropriately manage potential risks, it is important that you consider these e-discovery issues and have a plan in place to address them before sending your data off into the clouds.

Ben Barnett, chair of Dechert's mass torts and product liability practice, is an accomplished trial attorney. In addition to his trial work, he has extensive courtroom experience in a broad array of evolving e-discovery issues. For more than a decade, he has been the lead attorney responsible for coordinating nationwide discovery in several significant matters, many involving parallel proceedings. Regan Hunt Crotty's principal areas of practice are product liability and consumer protection litigation, with particular emphasis on class actions. As an associate in the firm's Princeton office, she has represented pharmaceutical and medical device manufacturers in litigation involving a cholesterol absorption inhibitor, diet drugs, and oral contraceptives.