How To Avoid Discovery Problems While Using The Cloud

Law360, New York (March 07, 2014, 1:28 PM ET) -- Cloud service providers offer remote access to networks, storage, hardware and computing services, giving users access to data through the Internet anytime, anywhere. By allowing businesses to outsource their information technology services, the flexibility and cost savings of cloud computing are revolutionizing the interaction between business and technology. The cloud computing industry was expected to reach $131 billion in annual revenues in 2013 — more than double the $58.6 billion in revenues in 2009.[1] Cloud technology is becoming popular because it dramatically decreases the cost of IT services while providing easier access to data.

While cloud computing affords considerable savings, it also creates hefty litigation concerns. Users and cloud providers alike may find themselves choosing between complying with either U.S. subpoenas or EU data protection laws — a legal rock and a hard place. Cloud computing also affects a user's ability to satisfy its document production obligations since the cloud is vulnerable to accidental data loss, security breaches and abrupt termination of service resulting in the permanent loss of data. Without immediate access to the servers, users are facing new challenges in fulfilling their discovery obligations.

Who Controls Documents in the Cloud?

Like paper documents and data stored on local computers or servers, data stored on the cloud is subject to discovery and the corresponding duty to preserve. Document requests generally apply to documents that are relevant to the legal proceeding and are within the requested party's "possession, custody, or control."[2]

This principle evolved in a paper world, but "possession, custody, and control" is less obvious when cloud service providers store data in cloud-based document management systems. Documents under the possession, custody, or control of a party or subpoenaed entity are potentially discoverable as long as the party or entity is within the court's jurisdiction. The location of the data may be irrelevant; numerous courts have compelled production of a party's information even though it was within the possession or custody of another entity outside the court's jurisdiction.[3]

While legal ownership and the conditions of access to documents normally are governed by the service contract between the user and the cloud service provider, courts may find that both the user and the cloud provider have control for the purpose of discovery.[4] Cloud computing allows users easy access to their documents — the user typically retains both the legal right and the practical ability to obtain the documents from the cloud. While the cloud provider operates as the middleman between the data and the user, it also takes custody of the data when it provides storage. Even if the service contract delineates possession, custody, and control or outlines discovery obligations, a court may decide that both the cloud service provider and the user must respond to production requests.

Cross-Border Litigation Risks in the Cloud

One of the principal advantages of cloud computing — that the actual location of the data is irrelevant because the data can be accessed from anywhere — gives rise to one of its biggest challenges: How can organizations that use cloud services housed in a foreign country ensure compliance with that country's data privacy laws? Due to the portable nature of electronic data, cloud data may migrate from one foreign jurisdiction to another, or be stored in multiple jurisdictions simultaneously.

Even though data is easily mobile, the location and use of the data affects a party's compliance obligations. For example, if the user engages the cloud provider because of or related to its establishment in the EU, the information stored in the cloud may be subject to EU data protection legislation.[5] Despite the barriers created by foreign data protection laws, some U.S. courts have ordered production of documents located outside the U.S., even though the transfer of such documents was forbidden by foreign law.[6]

In addition, U.S. courts have held that government concerns may outweigh international interests in protecting privacy.[7] If cloud providers and users who seek to obey EU data protection laws ignore subpoenas or court orders, U.S. courts may impose significant fines and other sanctions. This has created a tension between complying with U.S. litigation requirements and complying with EU data protection laws.

Document Preservation and Production Difficulties

Cloud computing may also increase the risk that the requested information will be deleted or lost. Cloud service providers frequently offer automatic deletion as part of their service package. Because federal courts have held that data in the possession of a third party may still be within the litigant's control, the litigant may be held responsible for any data stored in the cloud that is lost after the litigant has notice of the action even if the user made a timely request to the cloud service provider to suspend automatic deletion.

Data may also be accidentally lost if the cloud service provider experiences a crash or a security breach, the user fails to pay a bill, or the cloud provider goes out of business or otherwise terminates its cloud capabilities. Many end-user license agreements release the cloud provider from liability if data is lost for any reason. Although some jurisdictions will find spoliation only if there is intentional misconduct,[8] other jurisdictions may find spoliation on a showing of negligence.[9] Thus, a litigant may be subject to sanctions for spoliation if its information is accidentally lost, even if it issued a litigation hold.

The cloud also typically offers much more limited ability to search for and within documents. Normally, litigants can employ a forensic expert to search a hard drive and preserve electronically stored information. But because the cloud's servers are stored externally, are not under the direct control of the cloud user, and may be located all over the world, the user often is confined to simple searches for relevant terms. This type of

search is not nearly as extensive and may miss metadata and embedded information.

Finally, cloud provider services frequently include an automatic save function, which temporarily protects document drafts. These drafts each become their own document that is overwritten by the next auto-save. Each version is potentially discoverable, but cloud providers do not retain these draft files because they are quickly overwritten. When this type of data is stored on a computer, the shadow files of the previously auto-saved drafts are recoverable, but data stored in the cloud, especially public clouds, is so quickly overwritten that much of this data will be lost.[10]

Best Practices for Cloud Computing

As more people and businesses use the cloud, discovery of cloud data will become an important part of litigation. To prevent discovery problems, users should consider the following practices regarding their cloud use.

1. Identify Security Needs Before Utilizing the Cloud

Choosing to operate a private cloud will increase the security of private or confidential information. If users select public or community clouds, they should consider leaving private and confidential information on local servers or hard drives while taking advantage of the benefits of cloud computing.

2. Take Time Choosing a Service Provider

When a user engages a cloud provider with locations in many different regions, the user should take steps to restrict the location of its information to prevent data from entering or exiting regions with data protection laws. Users should insist that providers disclose the locations of their server facilities, including those used for overflow capacity and backup.

3. Utilize the Permissible Cross-Border Transfer Programs

If a company needs to avail itself of cloud service providers that store data in foreign jurisdiction, that company should take steps to protect itself from potential liability. To ensure compliance with foreign data privacy law while at the same time preserving the benefits of the cloud, organizations should avail themselves of the available cross-border data transfer programs: the Federal Trade Commission-administered Safe Harbor program, model contract clause agreements, and binding corporate rules.

4. Negotiate and Understand Service Agreements

The service agreement defines the provider's and the user's legal rights. A 2010 survey of 30 standard agreements used by cloud providers found that they were weighted toward the provider and often violated foreign data protection laws.[11] Terms of service are more likely to be negotiable for large users of private clouds, which offer increased

customization.

Whether negotiating a cloud service agreement, or shopping around for favorable terms, users should understand what services are offered. Services such as comprehensive search options, instant suspension of the auto-delete function, and preservation of metadata and embedded data will prove useful when responding to discovery requests.

5. Create a Preparedness Plan

Develop a strategy for putting a litigation hold on cloud data into place. Know who to contact on the cloud provider team and how to suspend auto-deletion and preserve all potentially relevant data. Understand how the provider's system works, what types of data it creates that might not be apparent to the user, how long data lives beyond its stated, required life, and how preservation and collection can be accomplished if and when it is needed.

6. Confer With Opposing Counsel

Once litigation has begun, confer with opposing counsel to limit the extent of cloud preservation and production. If you discuss the discovery difficulties related to cloud-stored data, you may be able to limit discovery requests to easily produced data rather than metadata and embedded data. This discussion may also demonstrate to the court reasonable efforts to satisfy foreign privacy laws while navigating discovery requirements.

Conclusion

The cloud is changing the way businesses and individuals interact with technology. It is a less expensive and more flexible alternative to traditional IT services, but it also creates new discovery challenges. Because litigation over discovery of data stored in the cloud is in the forecast, cloud users must know how to use the cloud responsibly to avoid later difficulties with document production.

—By Robert Keeling, Sarah Hughes Newman and Marisa West, Sidley Austin LLP

Robert Keeling is a partner and Marisa West is an associate in Sidley Austin's Washington, D.C. office. Sarah Newman is an associate in Sidley's Chicago office.

The opinions expressed are those of the author(s) and do not necessarily reflect the views of the firm, its clients, or Portfolio Media Inc., or any of its or their respective affiliates. This article is for general information purposes and is not intended to be and should not be taken as legal advice.

[1] Gartner Says Worldwide Cloud Services Market to Surpass $68 Billion in 2010, available online at http://www.gartner.com/newsroom/id/1389313 (last visited Jan. 16,

2014); Gartner Says Worldwide Public Cloud Services Market to Total $131 Billion, available online at http://www.gartner.com/newsroom/id/2352816 (last visited Jan. 14, 2014).

[2] "A party may serve on any other party a request … to produce … items in the responding party's possession, custody, or control." FED. R. CIV. P. 34(a)(1) (emphasis added).

[3] See Mt. Hawley Ins. Co. v. Felman Production, Inc., 269 F.R.D. 609, 618 (S.D.W.Va. 2010) (citing Afros S.P.A. v. Krauss-Maffei Corp., 113 F.R.D. 127, 129 (D. Del. 1986).

[4] Although "control" is a critical factor in discoverability, it is not necessarily dispositive. There are other significant factors that may limit discovery even where control is present (e.g., comity, statutory protections for stored communications, privilege, etc.). A full discussion of these factors is beyond the scope of this paper.

[5] Article 29 Data Protection Working Party, Opinion on Applicable Law, WP 179, at *21 (Aug. 2010).

[6] Steven C. Bennett, James M. Daley, Natascha Gerlach, Storm Clouds Gathering for Cross-Border Discovery and Data Privacy: Cloud Computing Meets the U.S.A. Patriot Act, 13 Sedona Conf. J. 235, at *9 (Fall 2012).

[7] See, e.g., Linde v. Arab Bank, PLC, 706 F.3d 92, 109 (2d Cir. 2013); AccessData Corp. v. ALSTE Techs. GmbH, No. 2:08cv569, 2010 WL 318477, at *2 (D. Utah Jan. 21, 2010); In re Vivendi Universal, S.A. Sec. Litig., 618 F. Supp. 2d 335, 343 (S.D.N.Y. 2009); Columbia Pictures Indus. v. Bunnell, No. CV 06-1093, 2007 WL 2080419, at *56-57 (C.D. Cal. May 29, 2007).

[8] E.g., the Eighth and Tenth Circuits require intentional misconduct. Menz v. New Holland N. Am., Inc., 440 F.3d 1002, 1006 (8th Cir. Mo. 2006); Estate of Trentadue ex rel. Aguilar v. United States, 397 F.3d 840, 862-863 (10th Cir. Okla. 2005).

[9] The Second Circuit follows a "culpable state of mind" standard. Residential Funding Corp. v. DeGeorge Fin. Corp. 306 F.3d 99, 108 (2d Cir. 2002).

[10] Id. at *15.

[11] Simon Bradshaw, Christopher Millard & Ian Walden, Contracts for Clouds: Comparison and Analysis of the Terms and Conditions of Cloud Computing Services, 19(3) Int'l J.L. & Info. Tech. 187, at *17-18 (2010).