

December 2010

Avoid the Rainy Day: Survey of U.S. Cloud Computing Caselaw

Cloud Computing, a computer networking model that gives users on-demand access to shared software applications and data storage, is becoming increasingly popular among businesses and individuals. For example, if you use Google's Gmail for email and calendaring, Snapfish for online photo sharing and storage, your business remotely stores data with a third-party server provider like Salesforce, or uses Windows Azure to create and host web applications and services, you're already "floating in the cloud." This alert surveys U.S. cases that have direct implications for cloud users.

I. Using a Cloud May Increase the Possibility That You Will Have to Fend Off a Lawsuit in Another State

In order to be sued in a state where you do not reside, or where your business is not incorporated or headquartered, the court must have personal jurisdiction over you, *i.e.*, the power to force you to come to court. In assessing whether a defendant has sufficient contacts with a particular state to be sued there, the use of a cloud computing program could expose you to greater risk of being sued successfully in that state. For example, one court held that if you maintain a virtual data room where prospective parties considering a merger with or acquisition of your company can review vital documents for due diligence purposes, and that virtual room is accessed by the aggrieved party from the state where suit was eventually brought, the virtual data room can serve as a contact for personal jurisdiction purposes. *Forward Foods LLC v. Next Proteins, Inc.*, 873 N.Y.S.2d 511, 2008 WL 4602345 (N.Y. Sup. 2008).

This decision shows that businesses and individuals alike must be aware that their use of a cloud can potentially increase the number of contacts they are found to have with a particular state, and thus raise their potential exposure to lawsuits in multiple forums.

II. As Judges Become More Tech Savvy, They Will Be More Willing to Recognize Your Right to Privacy for Data Stored in the Cloud

Once you use cloud computing for storage, one important consideration is whether you will lose your right to privacy in data stored in the "cloud" of servers which are owned by third parties. The dissenting opinion in *State v. Bellar*, 217 P.3d 1094 (Or. App. 2009), recognizes that in the current cloud age, people have an expectation of privacy for data stored in the cloud. As this opinion illustrates, as courts continue to become more computer-literate, it is likely that judges will afford privacy rights in data saved in the cloud. Nevertheless, in the meantime, businesses and individuals alike must realize that not all judges will respect the privacy of data stored with third parties.

III. Just Because Your Company Uses a Third Party to Store Data Does Not Mean That You Will Be Exempt From Having to Turn Over Information During the "Discovery" Phase of a Trial



Another important consideration when you are using cloud computing is that you may be forced into litigation to turn over data stored in the cloud. In *Columbia Pictures, Inc. v. Bunnell*, 245 F.R.D. 443 (C.D.Cal. 2007), the court found that the data in issue, which was being routed to a third party entity and received in that third party's server, was within the defendant's control by virtue of defendant's "ability to manipulate at will" how the data was routed. Proof of the defendant's ability to manipulate the data's route was found in the fact that, just one month prior to the court hearing, defendant rerouted the data from its own servers to those of the third party.

This case shows that it is increasingly difficult for companies to hide behind their third party data storage providers when fielding discovery requests, as courts find that the third party's servers are within the company's control. Similarly, in *Tomlinson v. El Paso Corporation*, 245 F.R.D. 474 (D. Colo. 2007), the district court held that an employer was in control of digital pension plan data and other documentation held by a third party record-keeper and thus could be compelled to produce the data and documentation.

IV. *Depending on the Circumstances, How You Use the Cloud Could Infringe on Copyrights*

Copyright infringement may result from a company's or individual's actions in using cloud computing. Like file-sharing companies who operated without the permission of the copyright owners of the content they shared, companies or individuals who use cloud computing to make unauthorized content available to Internet users may be liable for copyright infringement.

For example, in *Arista Records, LLC v. Usenet.com, Inc.*, 633 F. Supp. 2d 124 (S.D.N.Y. 2009), recording companies brought suit against UCI for operating a service which made copyrighted music available for download. The cloud at issue here was the USENET Network, "a global system of online bulletin boards" on which subscribers could post their own messages or files and download files posted by others. The district court ruled in favor of the record company, finding, among other things, that the defendants actively promoted copyright infringement by the cloud's users. The court's reasoning was based, in part, on the fact that it found "rampant" evidence of illegal music downloads occurring on the USENET, and evidence that copyrighted music had been uploaded to the cloud and illegally downloaded by its users.

V. *Cloud Wars: Providers Such as Microsoft and Google Compete to Provide Cloud Computing Services*

In what is undoubtedly a sign of things to come, Google and Microsoft are now battling for dominance in the cloud computing services market in the form of government contracts to provide those services.

In *Google v. The United States*, filed by Google in the U.S. Court of Claims in October 2010, the Department of Interior (DOI) sought a cloud service provider to outfit the agency with a single hosted email and collaboration services system in an effort to centralize its messaging services, which currently includes thirteen separate email platforms. Google believed that it could present a competitive offer with its Google Apps product, which it claims is the first suite of cloud-computing applications to receive Federal Information Security Management Act (FISMA) certification and accreditation.

But according to Google, despite repeated efforts at conveying their interest and the abilities of their cloud-product, the DOI focused on moving forward with a new Microsoft cloud-service, Business Productivity Online Suite-Federal (BPOS). Google's lawsuit claims that the Microsoft BPOS product is new and untested, as it has not been certified to meet FISMA standards. Google also asserts that the DOI's insistence on a "private cloud" for the Department, *i.e.*, their demand that the cloud's data storage and computing infrastructure be dedicated solely to the Federal government, is not necessary to satisfy the Department's needs.

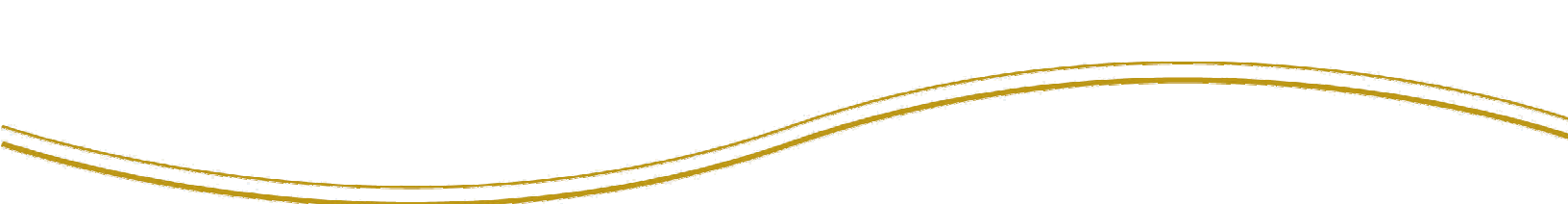


NJ: 721 Route 202-206, Suite 200 P.O. Box 5933 Bridgewater, NJ 08807-5933 • P: (908) 722-0700 • F: (908) 722-0755

NY: 875 Third Avenue, 8th Floor New York, NY 10022 • P: (212) 808-0700 • F: (212) 808-0844

PA: The Paragon Centre, Suite 300 1611 Pond Road Allentown, PA 18104-2258 • P: (610) 391-1800 • F: (610) 391-1805

www.nmmlaw.com E: info@nmmlaw.com



Believing that the seemingly pre-determined decision to move forward with Microsoft's BPOS was in violation of federal law, Google now seeks to prevent the DOI from continuing to proceed with its placement process with Microsoft, and seeks a court order requiring the DOI to hold an open and competitive bid process. With the market for cloud-based solutions on the rise, this is sure to be just one of many "cloud wars."

VI. Conclusion

Clearly, cloud computing remains a relatively new technology that will generate a variety of legal issues as time goes on. In the meantime, cloud-users should heed the lessons learned from early court decisions, and avoid the pitfalls of their predecessors. While the cloud can be a tremendous business tool, only time will tell how courts will perceive its use in terms of privacy rights, personal jurisdiction, and other important issues. It is hoped that these future decisions will help to advance technology while at the same time respecting the legal rights of those impacted by the use of cloud computing.

This *Internet Law Alert* was written by **Fernando Pinguelo** and **Bradford Muller**, of Norris McLaughlin & Marcus, P.A. If you have any questions regarding the information in this alert or any other related matters, please feel free to contact Fernando or Brad by email at fmpinguelo@nmmlaw.com or bwmuller@nmmlaw.com, respectively.

The *Internet Law Alert* provides information to our clients and friends about current legal developments of general interest in the area of taxation. The information contained in this Alert should not be construed as legal advice, and readers should not act upon such without professional counsel. Copyright © 2010 Norris McLaughlin & Marcus, P.A.



NJ: 721 Route 202-206, Suite 200 P.O. Box 5933 Bridgewater, NJ 08807-5933 • P: (908) 722-0700 • F: (908) 722-0755
NY: 875 Third Avenue, 8th Floor New York, NY 10022 • P: (212) 808-0700 • F: (212) 808-0844
PA: The Paragon Centre, Suite 300 1611 Pond Road Allentown, PA 18104-2258 • P: (610) 391-1800 • F: (610) 391-1805

www.nmmlaw.com E: info@nmmlaw.com