



## From LegalTech NY 2010: Taking Compliance and E-discovery to the Cloud

Feb 9th, 2010 | By Gregory P. Bufithis, Esq.

*This post is one of several summarizing our coverage of LegalTech New York 2010. For our other posts [click here](#).*



***Reported by: Scott Madsen, Esq. / The Posse List Editorial Staff***

Deborah Baron (Vice President, Legal & Compliance, Autonomy) moderated the session titled “Taking Compliance and E-discovery to the Cloud”. (For a video interview of Deborah discussing cloud computing with Ari Kaplan [click here](#)).

The panel participants: Jason R. Baron (Director of Litigation, National Archives and Records Administration & Co-Chair, The Sedona Conference Working Group on Electronic Document Retention & Production); Browning E. Marean (Partner, DLA Piper); Wayne Matus (Partner, Pillsbury); Karla Wehbe (Senior Information Resource Manager, Risk Management, Bechtel Corporation); and George Tziahanas (Vice President of Compliance, Autonomy).

### ***What is cloud computing?***

When the Internet started it was Web 1.0. Then the web evolved into what we have today, an interactive platform that is Web 2.0. You can take information and put it up, or host it, in the cloud. “The Cloud” is a euphemism for the Internet. The Cloud (and the irony is not lost on us) is ethereal and means different things to different people so the panel described in brief the National Institute of Standards and Technology (NIST) definition ([click here](#) for more on NIST). That full technical definition from NIST is as follows and provides the framework for your further understanding of cloud computing:

### *Definition of Cloud Computing:*

*Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model promotes availability and is composed of five essential characteristics, three service models, and four deployment models.*

### *Essential Characteristics:*

*On-demand self-service. A consumer can unilaterally provision computing capabilities, such as server time and network storage, as needed automatically without requiring human interaction with each service's provider.*

*Broad network access. Capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms (e.g., mobile phones, laptops, and PDAs).*

*Resource pooling. The provider's computing resources are pooled to serve multiple consumers using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand. There is a sense of location independence in that the customer generally has no control or knowledge over the exact location of the provided resources but may be able to specify location at a higher level of abstraction (e.g., country, state, or datacenter). Examples of resources include storage, processing, memory, network bandwidth, and virtual machines.*

*Rapid elasticity. Capabilities can be rapidly and elastically provisioned, in some cases automatically, to quickly scale out and rapidly released to quickly scale in. To the consumer, the capabilities available for provisioning often appear to be unlimited and can be purchased in any quantity at any time.*

*Measured Service. Cloud systems automatically control and optimize resource use by leveraging a metering capability at some level of abstraction appropriate to the type of service (e.g., storage, processing, bandwidth, and active user accounts). Resource usage can be monitored, controlled, and reported providing transparency for both the provider and consumer of the utilized service.*

### *Service Models:*

*Cloud Software as a Service (SaaS). The capability provided to the consumer is to use the provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through a thin client interface such as a web browser (e.g., web-based email). The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings.*

*Cloud Platform as a Service (PaaS). The capability provided to the consumer is to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages and tools supported by the provider. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly application hosting environment configurations.*

*Cloud Infrastructure as a Service (IaaS). The capability provided to the consumer is to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, deployed applications, and possibly limited control of select networking components (e.g., host firewalls).*

*Deployment Models:*

*Private cloud. The cloud infrastructure is operated solely for an organization. It may be managed by the organization or a third party and may exist on premise or off premise.*

*Community cloud. The cloud infrastructure is shared by several organizations and supports a specific community that has shared concerns (e.g., mission, security requirements, policy, and compliance considerations). It may be managed by the organizations or a third party and may exist on premise or off premise.*

*Public cloud. The cloud infrastructure is made available to the general public or a large industry group and is owned by an organization selling cloud services.*

*Hybrid cloud. The cloud infrastructure is a composition of two or more clouds (private, community, or public) that remain unique entities but are bound together by standardized or proprietary technology that enables data and application portability (e.g., cloud bursting for load-balancing between clouds).*

### ***Overall advantages and issues***

The panel delved into the advantages of the cloud, as well as some of the issues:

*Advantages:*

Shared resources, information, hardware, software and other resources can be delivered more rapidly and searched. The cloud is not just for outsourcing, large corporations use the cloud for their data centers combining their local LANs with the cloud to increase capacity, in other words, a hybrid cloud. This should lead to lower costs for data storage, searching and retrieval.

*Issues with the Cloud:*

There have also emerged critical yet not fully unexplored issues such as: (1) Preservation, retention and disposal of the data; (2) Control and Access; (3) Collections and Holds (how do you instigate a litigation hold? What about metadata?); and (4) Privacy — the use of the data, the location of the data both lead to privacy concerns.

In evaluating a service agreement for hosting in the cloud, Wayne Matus offered up some things to include in the terms of service: Use of data, Location of data, Encryption, No change of terms, Destruction, Ownership (assignment), Subpoena, Audit rights.

On the downside of cloud computing: security issues. Wayne Matus mentioned he is involved with a case where there are weekly security breaches and this is “not the best of all possible worlds”. He also said “There’s someone really smart sitting in Kazakhstan figuring out how to break through it.” Private clouds were mentioned as one possible solution to the security issue.

And control, possession and location in the cloud are issues to be looked at as well. Cloud computing promises a huge liberation of human creativity and communication; but can this precious space for our collaboration be kept open and free? Cloud computing is bringing with it “cloud capitalism”. Companies will make money from organising these clouds for us. Apple already is, with its iTunes cloud of music and its cloud of thousands of third-party apps to run on the iPhone. Cloud computing will also bring a kind of cloud culture: increasingly, we will express ourselves through these clouds of films, videos, pictures, books, stories and music.

### ***Should Lawyers use the Cloud?***

Browning Marean said that the genie is out of the bottle. This is a disruptive technology in that pre-cloud law firms knew where their data was, but now in the cloud — where is your data? A litigation hold is the biggest challenge in the cloud. Also, in the “pre-cloud” world you knew where (physically) your data was located. You knew which jurisdiction you were in. Now, where is the data? It is important because privacy laws in the US vs. the EU are different and we have recently seen in several court cases how problematic it becomes.

The Cloud cannot be used as a shield, the data must be accessible. See Phillip M. Adams & Associates, L.L.C., v. Dell, Inc. 2009 WL 910801 (D.Utah March 30, 2009) ([click here](#)). But just because your client’s data is in the cloud does not mean you don’t have to produce it. See [FRCP 34\(a\) ii](#) and [FRCP 26\(a\)1\(a\)\(ii\)](#). It appears that when people have to make the decision about retention they go overboard, creating more ESI, which leads to more e-discovery. (Which leads to the search for more vendors with culling, filtering, ECA, “predictive coding” capabilities)

An important cloud computing case mentioned by the panel:

*Flagg v. City of Detroit*, 252 F.R.D. 346 (E.D. Mich. 2008) Access [here](#) and commentary [here](#) FRCP 34(a) required production of data in the cloud from text messages sent or received by employees of the City using text messaging devices supplied by SkyTel (for the case [click here](#)).

And also what is being commonly referred to as “Zubulake 6” or the very recent *Pension Committee of the University of Montreal Pension Plan v. Banc of America Securities, LLC, et al.*, 05 Civ. 9016 (SAS) (S.D.N.Y. Jan. 15, 2010), ([click here](#)) although this case seemed to be mentioned in *all* the sessions. Members of the panel opined that the case may very well require litigation holds too early and lead to higher costs of litigation.

The [Galleon hedge fund case](#) was mentioned as well which involved insider trading and wiped out a \$6 billion dollar fund in a few hours after an indictment was announced. Audio, texts, email, docs, trade records — all in the cloud and all part of the ediscovery requested by regulators — touched many outside regulated industries and included such giants as IBM, AMP and others.

### ***Side Bar***

Jason R. Baron gave an interesting historical note on the Oliver North/Iran-Contra episode. It occurred when government policy was to not use email for official purposes. He contrasted that later with the Obama administration, which has emphasized transparency and reversed the government agency trend to the point now where the default is for the government is to store more records in the cloud. Then he gave the “Field of Dreams” scenario: “If the CIO builds it, the lawyers will come,” which corroborated what Deborah Baron said earlier, that the legal system is catching up to the increases in technology.

### ***Social Media***

Social networking/social media (SM) was discussed as well. It was mentioned that [FINRA Regulatory Notice 10-06](#) recognizes social networking and provides for extended bookkeeping requirements if social media is used for business purposes (note: this is for financial industries, which are heavily regulated). It was mentioned that SM is an emerging technology and that companies need a SM policy, and they need to enforce it. Each company is different and has its own culture and should have it’s own unique policy and address what SM is being used for. Browning Marean said “50 year-olds shouldn’t be setting the policies for the 20 and 30-year-olds of the organization” (although if you work for a start-up that usually is what happens) while earlier Jason R Baron quipped that he made a deal with his daughter that as long as she doesn’t de-friend him on Facebook he won’t de-ATM card her. Do these two statements attest to the generational gap that exists today in SM use?

For the Powerpoint from the presentation which shows all the subjects discussed [click here](#).

### ***Postscript:***

It was a good session, with lots of information. As cloud computing comes of age, our links to one another will be increasingly routed through a vast shared “cloud” of data and software. These clouds, supported by huge server farms all over the world, will allow us to access data from many devices, not just computers; to use programs only when we need them and to share expensive resources such as servers more efficiently. Instead of linking to one another through a dumb, decentralised network, we will all be linking to and through shared clouds.

The session could not accommodate all issues. For instance, whose clouds will these be? Cloud capitalism and cloud culture will not always be in harmony. The best way to understand the coming conflicts over the cloud is to look at the issues already being raised by some of the earliest applications. China, where Google is belatedly standing up for the principles of a cloud free from government interference, is the most immediate example.

But Google also has a more pragmatic, commercial motive. Gmail is a cloud service. Users do not store their messages on their own computers but in a remote cloud run by Google. (The Guardian newspaper recently junked its own, costly email service in favour of Google's enterprise-level Gmail offering.) If Google cannot maintain the integrity of the Gmail cloud, it does not have a secure service to sell. There will be many battles of this kind in years to come where corporations, citizens and governments struggle for control of the cloud.

An equally significant battle involving Google's influence over the cloud is being played out in a nondescript courtroom in New York, where the company has been defending its plans, devised with several university libraries, to create a cloud of more than 10m digital books. The question is: on what terms will Google make these available to readers and recompense their authors and publishers?

This shared cultural cloud will come at a price that is difficult to calculate. Google will acquire considerable power over the future of publishing and books – which books to include in the cloud and which not.

This dispute is a template for many others to come. Governments will also have their own views about these clouds, seeing in them threats to national culture (the French response); threats to security (the Chinese response) or threats to competition (the response of the US department of justice).

Thus, just as it is emerging, open cloud culture is threatened on all sides by vested interests of traditional media companies, hungry new monopolists and governments that are intent of reasserting control over the unruly web.

All of this deserves a more detailed examination and it will form the base for the cloud computing vBook The Posse List is writing in collaboration with several e-discovery vendors, law firms and IT experts. It will be made available for free via our collateral site **[The Electronic Discovery Reading Room](#)**. Look for our announcement in the coming weeks. If you'd like information about contributing or being a sponsor, email us at **[manager@theposselist.com](mailto:manager@theposselist.com)**

*Gregory P. Bufithis is the founder and chairman of The Posse List and its sister sites The Electronic Discovery Reading Room (<http://www.ediscoveryreadingroom.com>) and The Posse Ranch ([www.theposseranch.com](http://www.theposseranch.com)). He is also founder and chairman of Project Counsel ([www.projectcounsel.com](http://www.projectcounsel.com)).*