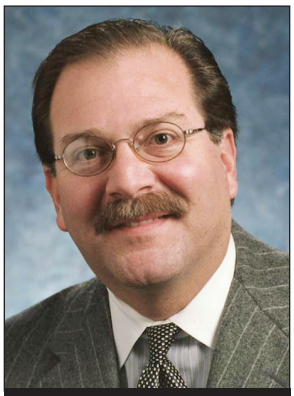
Connecticut Law Tribune
OCTOBER 11, 2010
VOL. 36, NO. 41 • $10.00
An ALM Publication
CTLAWTRIBUNE.COM

# Cloud Computing: Why Forecast Should Matter To You

## Storing data on Internet raises technological, legal issues

**By WILLIAM A. PERRONE, MARK W. HEAPHY and SARVESH D. MAHAJAN**


William A. Perrone


Mark W. Heaphy


Sarvesh D. Mahajan

On hearing the thunder of "cloud computing," one might expect to look to the sky and see a computer (about to fall). Yet the meaning and significance of "cloud computing" remain nebulous (pun intended).

"Cloud" is a metaphor for the amorphous Internet. In cloud computing, the Internet serves as the computer, combining software with infrastructure, a development platform, and databases. Cloud computing involves a shared pool of computing resources used in a multi-tenancy model. We all experience cloud computing when we use Google search or when we use web-based e-mail services such as Hotmail.

Cloud computing is viewed as a "greener" approach than current models. In particular, by running multiple applications on the same server (server virtualization), cloud computing provides dramatic gains in utilization of information technology resources, thus reducing the massive energy consumption of traditional computing devices.

Though the model is still in its infancy, most commentators anticipate cloud computing will be transformative. By moving the processing and storage of information to the cloud (rather than locally), the current models of computing may soon find their histories being written in the annals of computing alongside mainframe computing.

Such transformative events are often accompanied by uncertainty, and sometimes disruption. Cloud computing raises myriad technological, business, and legal issues. This article summarizes just some of the critical issues to consider while we wait for the cloud to bring "rain."

### Data Security

The paramount concern raised in most discussions of cloud computing is the security of data in the cloud. Physical security of the data centers is a basic question, though not unique to cloud computing. The multi-tenancy model of cloud computing creates multiple access points to applications. "Public" clouds (versus "private" clouds) may also create greater security risks.

Thus, operational security—the controls governing access to the applications, data, and the facility—requires close scrutiny. Additionally, the software-based controls, such as firewalls, encryption, and access rights, used by providers are essential component of provide a safe computing environment.

### Costs And Pricing Models

The promise of cloud computing is a high level of efficiency and scalability, and consequently, dramatic cost savings for customers. Even a large organization can now operate its entire business without investing in software, servers, and storage. Pricing for services delivered via the cloud have generally focused on subscription-type models. Pricing is tied to usage, for example, num-

*William A. Perrone is a Stamford-based partner in Wiggin and Dana's Technology and Outsourcing practice group. Mark W. Heaphy, who practices in New Haven, is chairman of the firm's Technology and Outsourcing group. Sarvesh D. Mahajan is an associate in the Technology and Outsourcing group, practicing in the firm's New York office.*

bers of users or transactions. These pricing models, combined with the cloud architecture, allow for significant variability in volume and a rapid scalability during times of high demand. Customers must remain vigilant to the other issues presented by the cloud computing model and not focus only on the dramatic cost savings.

## Maintenance And Support

Whereas the on-premise model of software typically requires customer to purchase separate maintenance contracts, maintenance for software in the cloud can be included in the subscription fees. By shedding fixed instances of software installed on servers, customers can have the benefits of fixes and upgrades instantaneously and continuously. On the other hand, Customers will also want to understand how they will receive support for information technology resources they do not control.

## Availability And Reliability

The speed and power of networks has allowed localized computing to spread across the network. Nonetheless, ensuring the same levels of reliability will be important for making the transition to cloud computing. Reliability and other measures of quality can be measured (and enforced) through a robust service level methodology and other performance metrics where customers can "keep vendors feet to the fire."

## Disaster Recovery

Of course, applications and data must be available when needed. So back-ups and redundancy are essential. By delegating responsibility of back-up and redundancy to the cloud provider, customers can eliminate the need for complex infrastructure as part of their business continuity planning.

## Intellectual Property, Licensing

Traditional software licenses are not compatible with cloud computing. Copies of software are not distributed locally. Rather cloud computing is service that is provided or made available to the customer. Moreover, much of the development of the cloud is based on "open source" material, creating additional challenges, not the least of which is ownership of data and intellectual property. Providers may be unwilling to provide broad indemnification protection as when they control and can neatly define the intellectual property they provide.

## Jurisdictional Issues

The dispersed infrastructure used by cloud provider creates a legal minefield for jurisdictional issues. The location and movement of data may lead various jurisdictions to assert regulatory authority and create conflicting obligations for customers and providers alike. By processing and storing in the cloud, customers must consider what new regulatory obligations they may be taking on. Some commentators consider the current legal landscape too risky to undertake cloud computing.

## Data Protection Laws

Many customers, and by extension providers, are subject to requirements under the Gramm-Leach-Bliley Act, the Health Insurance Portability and Accountability Act (HIPAA), Family Education Rights and Privacy Act (FERPA), and other applicable data protection and privacy laws. The numerous data protection regimes of various U.S. and international jurisdictions can pose significant hurdles when applied to the dynamic cloud architecture. Cross-border data flows are highly regulated, particularly in the international arena.

## Conclusion

While the business and legal world catch up to the cloud, parties interested in taking advantage of the "next big thing" will need to rely on strong contracting to allocate responsibility for the various risks presented by cloud computing. Currently, cloud computing is concentrated among a small group of powerful technology players, who may have sufficient to clout to dictate the terms of contract and design the rules of the emerging industry. Accordingly, customers should carefully understand exactly what they are buying and from whom in order to navigate this current trend which is growing at an incredible rate and is dramatically changing the information technology landscape. ■