Cyberspace Lawyer
June, 2009

CLOUD COMPUTING: THE INTERSECTION OF MASSIVE SCALABILITY, DATA SECURITY AND PRIVACY (PART I)

Barry Reingold, Ryan Mrazik [FNa1]

This article is the first in a three-part series that will look at cloud computing from the market and legal perspectives. This first article focuses on the technological and business capabilities of cloud computing and associated privacy and data security concerns. Part II will focus on the current state of the law that applies to cloud computing services. Part III will highlight industry and policy developments in the past months and upcoming few weeks.

Less than a year ago, at an Xconomy Forum entitled "The Promise and Reality of Cloud Computing," former IBM CEO Irving Wladawsky-Berger characterized cloud computing as the next evolution of the internet. [FN1] He also suggested that it would someday encompass billions of users and trillions of devices. [FN2] Dan Farber, editor in chief of CNET News, has said that we are only at the beginning of the "age of planetary computing." [FN3] In just the last few weeks, industry groups have called on information technology managers, government employees, users, and business leaders to cooperatively develop core principles for cloud computing and set standards for seamless integration of cloud computing systems across the globe. [FN4]

These comments and actions prompt many questions. What is cloud computing? Does cloud computing present any greater security risks than those in desktop-based or enterprise computing? What legal issues, such as jurisdiction, liability, and consumer protection, are associated with cloud computing? And finally, how will those issues affect individuals and organizations that use or provide cloud computing services?

Massive Scalability: Market Demand for Evolving Information Technology

"Cloud computing" refers to the development and use of Internet-based computer technology that allows users to access services without the need to control the infrastructure that provides the services. [FN5] Put simply, it's computing on demand that makes applications and storage from remote computers accessible anytime and anywhere. [FN6] Examples of common cloud computing services are services like Gmail and Hotmail that keep the users' e-mail messages on remote servers, rather than on the users' hard drives or on enterprise servers.

Cloud computing also encompasses more complex delivery mechanisms such as:

• "Software as a service" (SaaS) through which organizations rent third-party servers for highly intensive compilations or storage (BitTorrent) or desktop users access third-party servers to perform specific applications (Google Apps or Google Docs);

• Web 2.0 services that provide services such as social networking (Facebook);

• Cloud platforms, including on-demand platforms and "platform-as-a-service" (PaaS), which allow developers to write applications that run in and use services provided from the cloud (Amazon's Elastic Compute

Cloud); and

• "Infrastructure-as-a-service" (IaaS) that allows people to rent services such as processing, storage, network capacity, and other computing resources. [FN7]

Cloud computing services harness international networks of computing resources to provide scalable information technology services, including applications, processing, storage, technical support, and technical infrastructure. The third-party servers can be located anywhere in the world. And, the cloud computing service provider can shift data from one server to another depending on its immediate processing and storage needs. In some cases, the third party service providers may even contract with other providers for additional capacity on an as-needed basis. [FN8]

Since users can buy and use as much or as little computing, storage, processing, and development power as they need without having to invest in their own hardware, software, or information technology expertise, cloud computing has been labeled as "massively scalable." [FN9] Its resources can be custom fit to provide services for any computing task. The demand for and use of cloud computing services seems destined to expand.

Is the Cloud Safer Than Your Hard Drive?

As part of their services, cloud computing providers store and process massive amounts of data for their users. Privacy advocacy groups have suggested that cloud computing inherently poses greater risks than traditional desktop-based or enterprise computing, and that, until the security of data within the cloud can be verified, cloud computing services should be forced to adopt security features like mandatory encryption of all stored consumer data.

There is an ongoing debate about whether this is feasible. Suggesting that encryption is the answer to all cloud computing security issues ignores several issues. These include the need for innovation in this nascent industry; the desirability of customer choice; and the place for low-cost, simple cloud computing services in a market where users, based on their own needs, assess and choose what information to store remotely, what information to store locally, and what information not to store at all. Most cloud computing service providers offer encryption services during data transmission, but a request for encryption of stored data goes beyond the industry standard and may, because of technological constraints, degrade the services. [FN10]

On the broader issue of data security, the industry is still trying to get a better handle on the number of breaches and their seriousness. [FN11] Even with the relative youth of the cloud computing industry, those incidents do not seem to support a general conclusion about heightened security risks. In fact, cloud computing service providers argue the opposite: that cloud computing is more secure than desktop-based and enterprise computing. They point to:

• Built-in backups and safeguards that many desktop and enterprise servers do not have;

• The ability to make instant security upgrades available to all users (unlike desktop computing patches that seldom get downloaded or installed by users);

• Uniform high-end security to all users, regardless of size or industry;

• Technological expertise that few individuals or entities can match;

• Fragmentation, dispersal, and obfuscation of data across servers and platforms, making it unreadable by humans;

• Simplification of compliance analysis;

• Data held by an unbiased third-party with no motivation to wrongfully disclose;

• Lower-cost for disaster recovery and storage solutions; and

• Real-time detection of system tampering and on-demand security controls. [FN12]

Critics argue that these benefits, even if real, fail to recognize the relative youth of the cloud computing industry. These features, they contend, cannot substitute for an international data security standard and vigilant enforcement of cybercrime statutes. [FN13] In support of regulation or legislation explicitly governing cloud computing, they point to concerns, including:

• Reliance on private agreement between users and cloud computing service providers as the primary means of legal enforcement;

• The ability of cloud computing service providers to change terms of service with little or no notice to users of the service;

• An alleged lack of enforceable remedies against providers who suffer a data breach;

• The "monopolization" and integration of Web 2.0 and cloud computing services;

• The possible centralization of user data with a few cloud computing firms;

• Exposure of data to seizure by foreign government and data subpoenas; and

• The attraction to hackers of a "high value" target. [FN14]

This debate will continue to evolve with cloud computing technology and its use. Various industry and government groups are already beginning to coalesce to address these very issues. [FN15]

So, What's Next?

The debates surrounding cloud computing only raise more questions to consider:

• If standard terms of use are sufficient for downloading software or playing online games, why would they be inadequate for cloud computing services and applications?

• Given standard terms of use disclaimers that a product is not offered with any warranty to be error-free, how can critics seek to apply a strict liability standard when a bug or flaw appears and then results in a loss of data?

• Can a software bug or coding error be a deceptive trade practice in the cloud but business as usual when it's in a desktop or enterprise server?

• How will cloud computing services and the market for them continue to develop, especially in light of the emergence of industry forums and government interest that may demand higher levels of quality of service?

• How will the issue of jurisdiction evolve to cope with this new, international, interconnected network of computing resources? Whose law will apply to the service provider, the service, and the data?

• How can industry and market leaders best work with each other, regulators, and consumers to ensure that this massively scalable resource continues to evolve, addresses the needs of consumers, and achieves the necessary technical integration?

This list of questions only begins to scratch the surface of considerations that will likely come into play as cloud computing services continue to evolve and industry leaders, cloud computing users, regulators, and the legal community begin to address their benefits and challenges.

FNa1. Barry Reingold is a partner and Ryan Mrazik an associate in Perkins Coie LLP's Privacy and Data Security Practice. The views expressed in the article are those of the authors, and not Perkins Coie or its clients.

FN1. Irving Wladawsky-Berger, "Cloud Computing and the Coming IT Cambrian Explosion," Presentation at Xconomy 2008, slide 10 (2008) available at http:// www.xconomy.com/wordpress/wpcontent/images/2008/06/wladawskybergersmall.pdf (last accessed April 16, 2009).

FN2. Id.

FN3. Peter Mell and Tim Grance, "Effectively and Securely Using the Cloud Computing Paradigm," Presentation, NIST Information Technology Laboratory, slide 32 (March 13, 2009) available at http:// www.scribd.com/doc/13427395/Effectively-and-Securely-Using-the-Cloud-Computing-Paradigm (last accessed April 16, 2009).

FN4. See e.g., "Open Cloud Manifesto" available at http:// www.opencloudmanifesto.org/ (last accessed April 16, 2009) (manifesto stating that goal is to develop set of core principles for cloud computing) and "Cloud Computing Interoperability Forum" available at http://www.cloudforum.org/ (last accessed April 16, 2009) (forum to "enable a cloud cloud computing ecosystem ... for the purpose for wider industry adoption of cloud computing ...).

FN5. "Enterprise Cloud Services: Deriving Business Value From Cloud Computing," White Paper, MicroFocus, at 1 (2008) available at http:// cloudservices.microfocus.com/main/default.aspx/MFECS/White%20Paper.html (last accessed April 16, 2009).

FN6. Jeffrey F. Rayport and Andrew Heyward, "Envisioning the Cloud: The Next Computing Paradigm," at i (2009) available at http:// www.marketspaceadvisory.com/cloud/ (registration required; last accessed April 16, 2009).

FN7. MicroFocus, supra note 5, at 1; David Chappel, "A Short Introduction to Cloud Platforms: An Enterprise-Oriented View," at 3, 8 (2008) available at http://www.davidchappell.com/CloudPlatforms--Chappell.pdf (last accessed April 16, 2009); Mell and Grance, supra note 3, at slide 10.

FN8. Part II of this series will examine the legal issues that cloud computing raises under current law.

FN9. Wladawsky-Berger, supra note 1, at slides 10-11.

FN10. See e.g. Neil Roiter, "How to Secure Cloud Computing," Information Security Mag. (2009) available at http:// searchsecurity.techtarget.com/magazineFeature/0,296894,sid14_gci1349670, 00.html (registration required; last accessed on April 16, 2009) (noting that all service providers offer strong encryption during transmission, but that encrypting data at rest is more complex); see e.g. Zoho.com, "Zoho Security Practices, Policies & Infrastructure," available at http:// www.zoho.com/security.html (discussing encryption during transmission, but not while data is at rest) (last accessed April 16, 2009).

FN11. See "Customers Want Protection from Salesforce. com Breach." Computerworld, Nov. 9, 2007 available at http:// www.computerworld.com.au/article/198842/customers_want_protection_from_ salesforce_com_breach (discussing victimization of a cloud service following a phishing attack on an employee) (last accessed April 16, 2009).

FN12. Rayport and Heyward, supra note 6, at 35-37; Mell and Grance, supra note 7, at slides 22-23.

FN13. Rayport and Heyward, supra note 12, at 35, 38.

FN14. FTC Workshop, "Securing Personal Data in the Global Economy: Data Flows and Cross-Border Conflicts," Statement of EPIC Director Mark Rotenberg (2009), transcript and video available at http://htc-01.media.globix.net/COMP008760MOD1/ftc_web/FTCindex.html#Mar16_09 (last accessed April 16, 2009); Mell and Grance, supra note 12, at slides 24-25.

FN15. See e.g. "Open Cloud Manifesto," available at www.opencloudmanifesto.org and "Cloud Computing Interoperability Forum" available at www.cloudforum.org. (last accessed April 16, 2009). Part III of this series will examine these developments.

END OF DOCUMENT