The Information Technology
& Innovation Foundation

Cloud Computing Requires National Policy Leadership

BY DANIEL CASTRO | AUGUST 2010

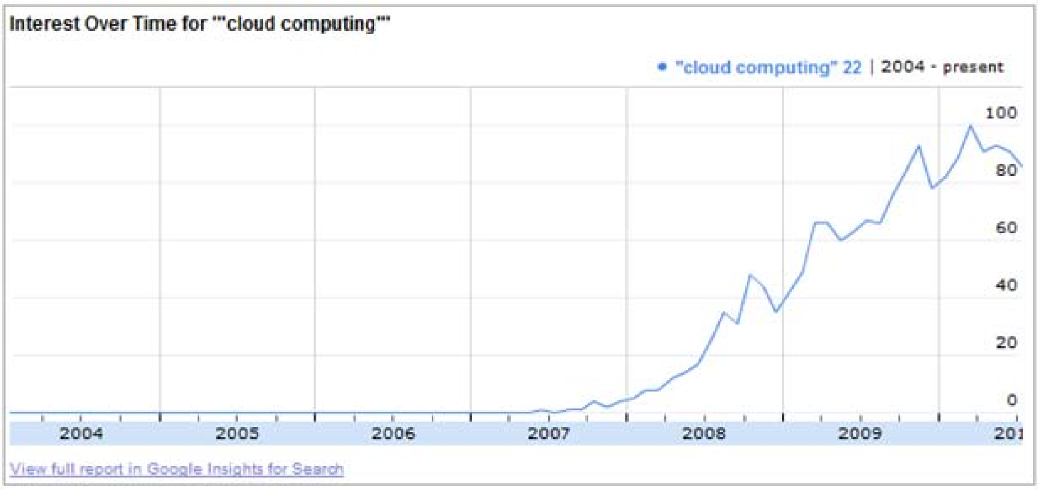
Policymakers should work both to ensure that the right policies are in place to enable widespread use of cloud computing and to resist anti-competitive policies pursued by other countries to challenge U.S. leadership in this sector.

Is “cloud computing” just the latest buzzword of the IT industry or the next big thing? The answer is that the truth lies somewhere in between. Cloud computing remains one of those terms, like “Web 2.0,” that is both overused and misused so often that the term has been rendered virtually meaningless. While marketers and start-ups may be hyping cloud computing, the term remains popular today because it describes a trend in computing that will have a significant effect on the development of new products and services for businesses, governments and individuals. Policymakers should be cognizant of these changes and work to ensure that the right policies are in place to enable widespread use of cloud computing. They should also resist anti-competitive policies pursued by other countries to challenge U.S. leadership in this sector, such as privacy laws or security regulations that unfairly advantage domestic firms.

CLOUD COMPUTING TODAY

As shown in Figure 1, interest in cloud computing has grown rapidly in the past two years. But while the term cloud computing has gained prominence only recently, its history can be traced back to the early days of computing when time-sharing environments were commonplace on IBM mainframes. But cloud computing goes beyond a mere client-server relationship which has existed since the early days of computing when dumb terminals interfaced with mainframes. Cloud computing represents IT as a service—software as a service, platform as a service, and infrastructure as a service.

Figure 1: Interest over time on Google for search term "cloud computing"[1]



The U.S. National Institute of Standards and Technology (NIST) defines cloud computing as "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."[2] Lewis Cunningham, an Oracle data architect defines cloud computing (more succinctly, but slightly less accurately), as "using the Internet to access someone else's software running on someone else's hardware in someone else's data center while paying only for what you use."[3]

A summary of the different types of cloud computing services is as follows:

- Software as a service (SAAS) is how most consumers today encounter cloud computing. Rather than run software locally on a PC they run the software in the cloud. Examples of SAAS include Google Maps for online mapping, Yahoo's Flickr for online photo sharing, Microsoft Hotmail for online email, or Intuit's Mint.com for online personal finance management.

- Platform as a service (PAAS) allows users to access a computing platform to develop or host online applications. For example, Google App Engine allows developers to create and run Web applications that run on top of a custom Google platform and uses Google's computing resources.

- Infrastructure as a service (IAAS) gives users access to virtualized computing resources that can be scaled to their needs. This allows companies to purchase computing resources on a metered basis, much like they would purchase electricity, water or any other utility. An example of IAAS is cloud storage such as Rackspace Cloud or Amazon Simple Storage Service (S3) which provides users access to scalable online storage. Similarly Microsoft's Windows Azure Platform provides pay-as-you-go pricing for computing, data transfers and storage.

For many consumers, the migration to cloud computing has gone unnoticed. Most people use cloud computing resources without even thinking about it. Services like Gmail, Facebook and YouTube epitomize the type of Internet-based applications users have come to expect as they increasingly rely on web-based services instead of local computing resources for their technical needs. Much of this change is driven by fast broadband connections, low-cost mobile devices and a mobile population that expects access to their data and applications anytime and anywhere.

Organizations are embracing cloud computing for many reasons. For one, cloud computing gives them flexibility. A business, for example, can scale up or down its IT usage according to demand. Organizations benefit from the agility that cloud computing offers them—no long-term commitments and no high sunk costs. Government agencies, for example, can better align cost with use by only paying for the actual use of IT resources for applications, rather than having to overbuild capacity based on potential demand. This agility also allows organizations to easily upgrade their applications as they can change platforms simply by switching cloud providers. This flexibility is especially useful for start-ups as they can focus on building applications rather than on building infrastructure which reduces a start-up's dependence on venture capital.

Cloud computing also allows organizations to focus on their core business and not their IT. Running data centers is hard, and organizations benefit from cloud computing because service providers can provide greater economies of scale, share resources across multiple customers, and provide higher levels of expertise in operating a secure, reliable, and energy-efficient data center. Cloud computing can be more efficient as most organizations, particularly small and mid-sized organizations, are not sufficiently large or sophisticated to take advantage of the economies of scale possible with IT.

There has been some debate about whether an organization should trust a third party to secure their data. Some people argue that large amounts of data in the cloud represent an attractive target for hackers and thus data in the cloud is more at risk than data stored elsewhere. However, arguing that data in the cloud is more at risk because there is more data is like arguing that because banks hold a large amount of money, and thus are an attractive target for bank robbers, people should not keep their money in banks. The fact is that for most people money in a bank is safer than money under a mattress, and the same is true in the cloud. While cloud computing does not guarantee security, and organizations should investigate the terms of service and security practices of any service provider, the general trend in cloud computing will likely lead to better overall security because implementing a good security program requires resources and expertise that many small and mid-sized organizations lack. Cloud computing represents an opportunity for these organizations to get better data security at affordable prices.

POLICY IMPLICATIONS, QUESTIONS AND RECOMMENDATIONS

While cloud computing reflects a new way for organizations to consume and manage IT, it has not created new policy questions, so much as it has highlighted the importance of existing ones. Chief among these are questions about jurisdiction and national sovereignty on the Internet.[4] Although any organization with a website has a global presence, it is unreasonable to expect organizations to comply with all of the laws and regulations of countries in which their connection does not go beyond a virtual one. Determining which rules apply to which organizations online is difficult and can become more complex when using cloud computing services that span national boundaries. However, these fundamental questions have existed for decades. While there are no easy answers here and it is unlikely that international harmonization will occur soon over issues as contentious as free speech, intellectual property, and electronic surveillance, a global conversation is needed now more than ever to create international agreements about jurisdictional issues surrounding data and services online.

Some people have also raised questions about the privacy of data stored in the cloud and the legal regime governing it. However storing data in the cloud does not reduce or limit the liability of an organization for ensuring the privacy of its data. An organization responsible for ensuring the privacy of its customer's data could be held liable for a breach of privacy regardless of if it occurs in the cloud or on its own local server. Questions of responsibility for ensuring the privacy of data between the organization who owns the data and the cloud computing service provider should be resolved through contract law. Again, this means that organizations should be clear about the terms of service they receive from cloud providers to ensure that they obtain the level of service they require. Consumers storing data in the cloud should also be clear about the terms of service and privacy policy offered by a service provider before storing their sensitive data online. Transparency is thus essential in cloud computing to ensure the market rewards good providers and penalizes bad ones.

While many of the policy questions are not new, policymakers can still help cloud computing flourish by creating policies that will support its development and avoiding policies that will hinder it. With this in mind, we recommend policymakers follow two basic principles to encourage continued U.S. leadership in cloud computing:

1. Create "cloud-neutral" policies

Laws and regulations should not be created to either favor or disfavor cloud computing. One of the principal areas of law that needs to be updated in the United States relates to electronic surveillance of data. The Electronic Communications Privacy Act (ECPA) was enacted in 1986 and has not kept pace with the advancement of technology. For example, there are different levels of protection afforded to the privacy of an individual's data based on where the data is stored and how long the data has been stored. This means that the privacy of a person's email may be different if it is stored on his or her PC versus if it is stored in the cloud. In the former case law enforcement might need a search warrant based on probable cause to review the data, but in the latter law enforcement would only need a subpoena.[5] Consensus seems to be forming that reform is needed in this area to protect Fourth Amendment rights. Where possible, the privacy of an individual's communication should be the same regardless of the type of technology that is used to facilitate this communication.

Similarly policymakers should strengthen laws such as the Computer Fraud and Abuse Act (CFAA) to establish greater penalties and make it easier to prosecute criminals who hack into cloud computing services. This would include, among other things, changing the CFAA to make penalties correspond to the number of accounts illegally accessed on an online service rather than limit them to the penalties for hacking into a single PC.[6] Creating "cloud-neutral" policies will also require changes such as government leaders ensuring that their procurement practices do not exclude cloud computing services or favor non-cloud services. Finally, it also means that while policymakers should encourage competition in the marketplace and look out for the interests of consumers, they should avoid heavy-handed regulations specific to cloud computing in the name of privacy, security, interoperability or some other goal. Instead, policymakers should use a light touch to encourage greater industry self-regulation, transparency and best practices.

2. Resist mercantilist policies

Restrictions on the global flow of data limit economic activity by imposing costs on commerce and communication. Policymakers should work to ensure that cloud computing does not become balkanized because of nationalist legal restrictions imposed by other countries. Analysts predict that cloud computing will comprise approximately $42 billion of IT budgets worldwide by 2012.[7] Currently, the United States is one of the primary providers of cloud computing services, however many other nations are vying to be the leader in this field. While competition is healthy, policymakers should be vigilant about identifying mercantilist policies erected by other countries that intentionally disadvantage foreign businesses. For example, countries may create geographic restrictions on where providers can store data, use data security or privacy laws to disadvantage foreign firms, or impose green data center requirements that unfairly favor domestic firms over foreign competitors.[8]

Where possible the United States should avoid these policies itself otherwise it risks losing credibility on the international stage. For example, the City of Los Angeles began using Google Apps across its organization but first required that Google create a special "Google Apps for Government" cloud service which restricted data from being stored outside of the United States. If other countries implement similar policies, U.S.-based cloud computing service providers have the most to lose as the domestic market for cloud services is much smaller than the global market. The goal should be to work towards eliminating geographic restrictions on the flow of data across borders.

CONCLUSION

Cloud computing will likely continue to grow as more users flock to this computing paradigm and as legacy systems are retired and organizations shift towards outsourcing more of their IT. Policymakers would be wise to recognize the value of this opportunity and ensure that business can use and sell cloud computing services without undue burdens.

ENDNOTES

[1] "Google Insights for Search: Cloud Computing," Google, accessed on July 30, 2010. http://www.google.com/insights/search/#q=%22cloud%20computing%22&cmpt=q

[2] Peter Mell and Tim Grance, "NIST Definition of Cloud Computing, Version 15" National Institute of Standards and Technology, October 7, 2009, http://csrc.nist.gov/groups/SNS/cloud-computing/.

[3] Lewis Cunningham, "Cloud Computing Defined," November 21, 2008, http://it.toolbox.com/blogs/oracle-guide/cloud-computing-defined-28433.

[4] Shane Ham and Robert D. Atkinson, "A Third Way Framework for Global Ecommerce," Progressive Policy Institute, March 15, 2001, http://www.ppionline.org/ppi_ci.cfm?knlgAreaID=140&subsecID=292&contentID=3156.

[5] For more on this issue, see the Digital Due Process Coalition, www.digitaldueprocess.org.

[6] See similar proposal in "Building Confidence in the Cloud: A Proposal for Industry and Government Action to Advance Cloud Computing," Microsoft, January 2010, http://www.microsoft.com/presspass/presskits/cloudpolicy/.

[7] "Investors bet $110 million on clouds," Red Herring, March 28, 2010, http://www.redherring.com/Home/26330.

[8] For example, the German Data Protection Authority of the federal state of Schleswig-Holstein recently issued a legal opinion that many uses of cloud computing are in violation of German data privacy laws. See "Datenschutz bei Cloud Computing? Bisher Fehlanzeige!" (in German), Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein, June 18, 2010, https://www.datenschutzzentrum.de/presse/20100618-cloud-computing.htm.