Daniel Castro

Senior Analyst

Information Technology and Innovation Foundation (ITIF)

"Cloud Computing: An Overview of the Technology and the Issues Facing American Innovators"

Before the

Committee on the Judiciary

Subcommittee on Intellectual Property, Competition and the Internet

July 25, 2012

Chairman Goodlatte, Ranking Member Watt and members of the Subcommittee, I appreciate the opportunity to appear before you to discuss cloud computing and the opportunities and challenges presented by this technology. My name is Daniel Castro. I am a senior analyst at the Information Technology and Innovation Foundation (ITIF). ITIF is a nonpartisan research and educational institute whose mission is to formulate and promote public policies to advance technological innovation and productivity.

In my testimony today, I would like to provide an overview of some of the benefits of cloud computing and then focus my remarks on two important principles for cloud computing: 1) creating "cloud-neutral" policies and 2) addressing anti-competitive foreign practices that challenge the dominance of cloud computing service providers in the United States.

An Overview of Cloud Computing Technology

Cloud computing refers to the growing practice of selling IT as a service that is delivered over the Internet. The most common forms of cloud computing include software as a service (SaaS), platform as a service (PaaS), and infrastructure as a service (IaaS).

Software as a service (SaaS) is widely used by Internet users in the United States, such as to access web-based email or to share documents online. Users can access these applications online through a web browser on a PC or mobile device, rather than through software installed and run on a local desktop or server. Many of the most popular cloud-based applications are business productivity tools such as email (e.g., Gmail, Hotmail), online productivity software (e.g., Google Docs, Microsoft Office 365), conferencing services (e.g., Microsoft LiveMeeting, WebEx), and customer relationship management software (e.g., Salesforce).Using SaaS, customers can access software on-demand and pay for it on a metered basis, such as based on the level of usage or the number of users. Alternatively, there are many applications available at no-cost to users, and many of these are supported by ad-revenue.

Platform as a service (PaaS) allows users to rent virtualized software development or production environments ("platforms") to run their own applications or services. Organizations use PaaS to rapidly and efficiently develop and deploy new applications without having to invest in expensive hardware or software, or manage complex networking and computing infrastructure. PaaS can automate many complicated administrative technical functions, such as creating backups or test environments, and allow organizations to focus their resources on product development. PaaS also allows organizations to more easily scale up or down a computing environment to meet their computing needs for a particular application. 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 organizations of any size access to secure, enterprise-class computing infrastructure that can be efficiently managed and scaled to meet different 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, which provides users access to scalable online storage. Other IaaS approaches offer pay-as-you-go pricing for computing, data transfers and content distribution networks.

Cloud computing can be deployed in one of at least four different configurations: a private cloud, a community cloud, a public cloud, and a hybrid cloud. A private cloud is used exclusively by one organization with multiple business units and may be deployed either on-site or off-site. A community cloud is used exclusively by a specific group of organizations, often those sharing similar business interests or goals. For example, a community cloud may be provisioned for a group of federal agencies. In contrast to a private or community cloud, a public cloud is available for use by the general public. Lastly, a hybrid cloud refers to deploying an application or service across cloud computing infrastructure spanning two or more configurations (private, community, and public).[1]

Cloud computing has profoundly changed the economics of IT investments. In the previous model of computing, an organization would estimate how much computing power it needed, and then purchase the number of servers required to meet its peak needs. Most of the time, however, these computing resources would be underutilized. In addition, if an

organization's needs exceeded its estimates, the organization would have to scramble to purchase and bring online more servers.

Cloud computing eliminates many of these challenges. It creates a more flexible environment that allows organizations to "rent" computing power on an as-needed basis—an organization can scale up or down its IT usage according to demand. Organizations also benefit from the agility that cloud computing offers them as they have no long-term commitments and no high-fixed costs. Government agencies, for example, can better align cost with use by only paying for their actual use of IT resources, 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 also useful for start-ups as it enables them to focus on building applications and services rather than on building a costly IT infrastructure. The concepts behind cloud computing—on-demand, scalable and pay-per-use—make it ideal for applications that have variable demand for resources or need to be scalable.

Cloud computing will involve significant changes in IT infrastructure for businesses in the coming years. For example, Gartner estimates that by next year sixty percent of server workloads will be virtualized.[2] Similarly a McKinsey survey of 250 chief information officers (CIOs) of large companies across different industries found that they expect over two-thirds of corporate applications to be virtualized by 2014.[3] Virtualization cuts the cost of computing by up to 50 percent with savings gains from lower infrastructure operational costs. Not only are legacy applications being virtualized, new IT investments are predominantly in cloud computing. IDC estimates that 80 percent of new commercial applications deployed this year will be on cloud computing platforms.[4]

Cloud computing allows organizations of any size to focus on their core business and not their IT. Running data centers—buying, installing, operating, maintaining, and upgrading servers—is resource intensive. 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. In particular, cloud computing has been a boon to startups as it reduces their need for capital investments to build, run and maintain IT infrastructure. As the CEO of one cloud computing startup noted, "Cloud computing has done to hardware what open source has done to software."[5] The availability of low-cost cloud computing infrastructure allows startups to create products without having to make a heavy investment in IT infrastructure. Instead, they can scale to meet their user needs as they grow. Unlike existing firms, which must integrate cloud computing with legacy IT systems, startups can start fresh.[6]

Create Cloud-Neutral Policies

Every technology creates new challenges. While some concerns have been raised about cloud computing, especially those relating to security and privacy, there is no need to create cloud-specific regulations. For example, cloud computing does not reduce an organization's responsibility for protecting its data. Storing data in the cloud instead of on an organization's own local servers 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. 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.

Some concerns have also been raised about the privacy of data stored in the cloud and the legal regime governing it. In particular countries, especially some European countries, have argued that the Patriot Act gives the U.S. government more access to data stored by cloud computing service providers based in the United States than other governments have for cloud computing providers in their jurisdictions. While this is untrue, foreign competitors use this common misperception to seek an advantage over U.S.-based cloud computing service providers. As documented in a recent white paper by Hogan Lovells "it is incorrect to assume that the United States government's access to data in the Cloud is greater than that of other advanced economies."[7] In fact, the United States actually has more legal protections for some data stored in the cloud than other countries. For example, the United States has more restrictions on the voluntary disclosure of data stored in the cloud to government officials than in countries like Australia and Canada.[8] In addition, the existence of Mutual Legal Assistance Treaties (MLATs) between many countries means that many governments have the ability to obtain data stored outside of their jurisdiction.

Policymakers will eventually need to more thoroughly address the complex issues that come into play when data subjects, data owners, and service providers are under different legal jurisdictions and face conflicting regulations. These issues are not unique to cloud computing, but addressing these challenges will help simplify the regulatory complexity of using this technology. Meaningfully addressing jurisdictional issues may eventually require countries to

come to agreement on questions of jurisdiction or standardize some data practices. Alternatively, advances in technology that allow data policies to be bundled with data, and ensure that these policies are enforced, may also eventually help address some of the jurisdictional conflicts relating to cloud computing.

There has been some debate about the security of data stored in the cloud. Some people have argued 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 of it" 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 individuals (and companies) money in a bank is safer than money under a mattress, and the same is true in the cloud. The reason for this is simple: because of their targeted focus and advantages in scale, cloud computing companies are able to develop expertise in secure computing that other companies cannot easily match. While cloud computing does not guarantee security, and organizations should investigate the terms of service and security practices of any particular service provider, the net result of a shift towards greater use of cloud computing in the United States will likely be a decrease in the overall security risk profile for many U.S. companies. In particular, this is true for small and mid-sized organizations that lack the required resources and expertise to implement a strong security program. Cloud computing represents an opportunity for these organizations to get better data security at affordable prices.

Creating "cloud-neutral" policies will require some changes to ensure that laws and regulations do not favor or disfavor cloud computing. One important step Congress can take in this direction is to update the laws that govern the electronic surveillance of data. The Electronic

Communications Privacy Act (ECPA) was enacted in 1986 and has not kept pace with the advancement of technology and the growth of cloud computing. As a result, there are different levels of legal 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 right of the government to access 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.[9] However, the legal protections provided for an individual's private communications should not depend on the technology used to facilitate this communication. Consensus is forming that reform is needed in this area to protect Fourth Amendment rights.

Similarly policymakers should strengthen laws such as the Computer Fraud and Abuse Act (CFAA) which were written before cloud computing became widespread. Strengthening the CFAA would make it easier to prosecute criminals who hack into cloud computing services and establish penalties more in line with the impact of an attack. For example, CFAA should be changed 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.[10] This will bring penalties more in line with the impact of such an attack.

Anti-Competitive Foreign Practices Threaten U.S. Cloud Computing

Not only have U.S. firms like Amazon, Rackspace, and Google pioneered cloud computing services, U.S. firms currently dominate the cloud computing market. As some of the primary providers of cloud computing technology, U.S. companies have tremendous potential for growth as cloud computing adoption increases worldwide. Worldwide adoption of cloud

computing is growing rapidly. On the low end, the International Data Corporation (IDC) estimates that the global market for cloud computing will grow to $56 billion by 2014. American Megatrends, Inc. (AMI) research predicts that the market for cloud computing will reach $100 billion by 2014 for small and medium businesses alone.[11] Forrester Research predicts that the market for cloud computing will grow from approximately $41 billion in 2011 to $241 billion in 2020.[12] Software as a service is expected to make up the bulk of this market at approximately $133 billion in 2020 worldwide.[13] IDC estimates that spending on cloud computing services will generate almost 14 million jobs worldwide between 2011 and 2015, including over 1 million jobs in the United States.[14]

Although U.S. firms are the leading providers of cloud computing services, other countries are aggressively challenging U.S. leadership in this market. For example, in April 2012 the French government announced it was funding one-third of a €225 million joint venture with two French telecom and technology companies, Orange Telecom and Thales, to create a new cloud computing company. This company will provide processing, storage, and bandwidth cloud computing services to French and European companies.[15] In May 2012, the French government announced a second joint venture of equal value to fund another company with SFR and Bull that will also provide cloud computing services.[16] China is similarly competing to create an internationally competitive domestic cloud computing industry. The Beijing government built a 7,800 square meter complex dubbed "Cloud Valley" and offers cloud computing companies tax-breaks and low-cost office space to locate in Beijing. The Chinese government is also allowing some firms to apply for a direct Internet connection to bypass the country's censorship system and access foreign servers so that foreign companies can outsource IT services to China.[17]

While some state-based efforts to promote domestic industries are legitimate (or semi-legitimate), others are clearly not. Fair competition in the market is healthy, but policymakers should be vigilant about identifying mercantilist policies enacted by countries to intentionally disadvantage foreign competitors. In fact, "cloud mercantilism"—the adoption of a wide array of policies and restrictions focused on import substitution for cloud computing services—is an emerging threat to global trade in information technology. And what makes this problem more challenging is that many nations use the guise of privacy and security to defend what are at heart mercantilist policies.

Some countries use data security and data privacy regulations to create geographic restrictions on where cloud computing service providers can store and process data. Restrictions on the cross-border flow of information diminish the ability of service providers to distribute data over a diverse geographic region to ensure redundancy and increase reliability, an important benefit of cloud computing. Other countries have policies that explicitly require cloud computing service providers to operate data centers domestically. Localization requirements have the effect of making cloud computing less efficient, since data center siting decisions must be made based on political mandates rather than technical or economic factors. Localization requirements also serve as a form of protectionism for domestic cloud computing providers since it may not be economically viable for a foreign competitor to build a new data center.

Examples of this type of behavior can be found in many countries. For example, Greece, Vietnam and Brunei have all passed laws which require data generated within the country to be stored on servers within the country.[18] Both the Norwegian and Danish Data Protection Authorities have issued rulings to prevent the use of cloud computing services when servers are not located domestically.[19] The Ministry of Communications and Information in Kazakhstan

issued an order to require that all .kz domain names operate on servers located within the country. The government later modified this order so that it only applied to new domains, rather than existing domains, however, this type of policy still unfairly discriminates against foreign providers.[20] China has implemented local data server requirements ostensibly to protect national security and control currency. Russia, Venezuela and Nigeria have all passed regulations requiring that IT infrastructure for payment processing be located domestically.[21] And similar types of laws are pending in other countries including Indonesia, Malaysia and Ukraine.

Other countries have flirted with various policies to advantage domestic firms or at least try to capture the economic benefits of constructing and operating a data center. For example, India has proposed a measure to require companies to locate their IT operations within the country so that law enforcement and national security agencies can obtain data stored on their servers.[22] And in Australia, legislation was proposed that would require that local data centers be used to store data in its electronic health record system.

The principles to combat these types of practices already exist. Under *The European Union-United States Trade Principles for Information and Communication Technology Services*, a set of principles agreed to by the Office of the U.S. Trade Representative and the European Commission, this type of behavior would be clearly prohibited. First, the principle on cross-border information flows states, "governments should not prevent service suppliers of other countries, or customers of those suppliers, from electronically transferring information internally or across borders, accessing publicly available information, or accessing their own information stored in other countries." Second, the principle on local infrastructure states, in part, "Governments should not require ICT service suppliers to use local infrastructure, or establish a local presence, as a condition of supplying services."[23]

In short, strong U.S. leadership is necessary to combat unfair trade practices that other nations are using to block foreign competitors in the rapidly growing cloud computing industry. First, the U.S. government should clearly and definitively state its opposition to local data server requirements and highlight instances of non-compliance by foreign governments. U.S.-based cloud computing service providers will have the most to lose if localization requirements become widespread. After all, the domestic market for cloud services is much smaller than the global market. Even today, Latin American and Asian companies are adopting cloud computing at higher rates than in the United States.[24]

Second, the U.S. government should affirm its intention to refrain from imposing its own local data center requirements. These policies may be tempting, especially for government procurement of cloud computing services. For example, when the City of Los Angeles negotiated to use Google Apps across its organization, it first required that Google create a special "Google Apps for Government" cloud service which restricted data from being stored outside of the United States.[25] While such requirements may at times serve short-term interests, they diminish the capacity of the United States to hold other countries accountable for similar forms of protectionism. The United States should avoid these types of policies otherwise it risks losing credibility on the international stage. The long-term goal of the U.S. government should be to work towards eliminating geographic restrictions on cross-border flow of data.

At the same time, if the United States is going to seek the moral high ground on free trade in cloud services, it will have to amend ECPA as described above and ensure that government policies do not treat cloud computing differently than any other information technology.

Thank you for the opportunity to share with you my thoughts on cloud computing. I look forward to answering any questions you have.

Endnotes

1. Peter Mell and Timothy Grance, "The NIST Definition of Cloud Computing," SP 800-145, National Institute of Standards and Technology, September 2011, http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf.
2. Ryan Nichols, "Cloud computing by the numbers."
3. Prashant Gandhi, Gary Moe and Kara Sprague, "Where the cloud is likely to grow," McKinsey Global Institute, 2012.
4. Derrick Harris, "It's cloud prediction time," GigaOm, December 1, 2011, http://gigaom.com/cloud/its-cloud-prediction-time-idc-gartner-and-i-weigh-in/.
5. Christopher Calnan, "Cloud computing bursting on the corporate scene", Mass High Tech, August 1, 2008, http://www.masshightech.com/stories/2008/07/28/weekly8-Cloud-computing-bursting-on-the-corporate-scene-.html.
6. Jonathan Boutelle, "How Cloud Computing Impacts the Cash Needs of Startups," Gigaom, August 16, 2010, http://gigaom.com/cloud/how-computing-impacts-the-cash-needs-of-startups/.
7. Winston Maxwell and Christopher Wolf, "A Global Reality: Government Access to Data in the Cloud," May 23, 2012, http://www.hoganlovells.com/files/Publication/80a807f2-e619-41dc-98e4-e6a7b5f6c5f8/Presentation/PublicationAttachment/0fc74c1d-4dc0-4c1e-9abc-eb50ae5679c4/Hogan%20Lovells%20White%20paper%20-%20Government%20access%20to%20data%20in%20the%20cloud.pdf.
8. Ibid.
9. For more on this issue, see the Digital Due Process Coalition, www.digitaldueprocess.org.
10. 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/.
11. Ryan Nichols, "Cloud computing by the numbers: what do all the statistics mean," ComputerWorld, August 31, 2010, http://blogs.computerworld.com/16863/cloud_computing_by_the_numbers_what_do_all_the_statistics_mean.
12. "Cloud computing market: $241 billion in 2020," ZDNet, April 22, 2011, http://www.zdnet.com/blog/btl/cloud-computing-market-241-billion-in-2020/47702.
13. Ibid.
14. "Cloud Computing to Create 14 Million New Jobs by 2015," Microsoft News Center, March 5, 2012, http://www.microsoft.com/en-us/news/features/2012/mar12/03-05CloudComputingJobs.aspx.
15. "Orange and Thales welcome French State support for their joint project Andromède," Press release. April 20, 2012 http://www.thalesgroup.com/Press_Releases/Markets/Security/2012/20120420_DSC_Orange_and_Thales_welcome_French_State_support_for_their_joint_project_Androm%C3%A8de/.
16. "Vivendi's SFT and Bull Form Cloud Computing Company, Echos Says," Bloomberg, May 10, 2012, http://www.bloomberg.com/news/2012-05-10/vivendi-s-sfr-and-bull-form-cloud-computing-company-echos-says.html.
17. "Beijing hopes to dominate cloud computing with 'Cloud Valley,'" Smart Planet, December 16, 2011, http://www.smartplanet.com/blog/global-observer/beijing-hopes-to-dominate-cloud-computing-with-8220cloud-valley-8221/1313.
18. "Promoting Economic Growth through Smart Global Information Technology Policy," Business Roundtable, June 2012, http://mercatorxxi.com/merc/wp-content/uploads/2009/07/Global-IT-Policy-Paper-final.pdf.
19. See for example, "Processing of sensitive personal data in a cloud solution," February 3, 2011, http://www.datatilsynet.dk/english/processing-of-sensitive-personal-data-in-a-cloud-solution/ and "Will Not Let Norwegian Enterprises use Google Apps," January 25, 2012, http://datatilsynet.no/English/Publications/Will-not-let-Norwegian-enterprises-of-Google-Apps/.
20. "Changes to the Open Internet in Kazakhstan," Google Blog, June 7, 2011, http://googleblog.blogspot.com/2011/06/changes-to-open-internet-in-kazakhstan.html.

21. Ibid.
22. "Promoting Economic Growth through Smart Global Information Technology Policy," Business Roundtable, June 2012, http://mercatorxxi.com/merc/wp-content/uploads/2009/07/Global-IT-Policy-Paper-final.pdf.
23. "European Union-United States Trade Principles for Information and Communication Technology Services," April 4, 2011, http://ec.europa.eu/information_society/activities/internationalrel/docs/eu-us-tradeprinciples.pdf.
24. "The State of Adoption of Cloud Applications," Tata Consultancy Services, March 26, 2012, http://sites.tcs.com/cloudstudy/the-state-of-adoption-of-cloud-applications#.UAyxd7RfE4m.
25. An online help page for Google Apps for Government currently states that "Customer email and calendar data is stored only in facilities in the continental United States (CONUS)." Source: "Google Apps for Government," Google.com, n.d., http://support.google.com/a/bin/answer.py?hl=en&answer=174120 (accessed July 22, 2012).