

Mr. Daniel Chenok
Executive Director
Center for The Business of Government
IBM

House Judiciary Subcommittee on Intellectual Property, Competition, and the Internet
"Cloud Computing: An Overview of the Technology
and the Issues facing American Innovators"
July 25, 2012

Good afternoon, and thank you Chairman Goodlatte, Ranking Member Watt, and the entire Subcommittee for the opportunity to speak with you about cloud computing.

I am Dan Chenok, Executive Director of the Center for The Business of Government at IBM. The Center connects public management research with practice. Since 1998, we have helped public sector executives improve the effectiveness of government with practical ideas and original thinking. We sponsor independent research from the academic and non-profit sectors, and we create opportunities for dialogue on a broad range of public management topics. The Center has addressed cloud computing from a number of perspectives over the past few years.

I also serve as Chair of the Information Security and Privacy Advisory Board, which is chartered under the Federal Information Security Management Act (FISMA) to advise the government about information security and privacy issues affecting civilian Federal agencies, and has addressed security and privacy issues involved in cloud computing. My testimony today draws on this and other experience that I have had with the growth of cloud computing, primarily with respect to how government can best promote the efficient, secure, and cost-effective use of this technology. After addressing context and benefits, I will focus on three key issues that impact how cloud can best be leveraged, now and in the future.

Context

Many descriptions of cloud computing are cited across government and industry, including a formal definition from the National Institute of Standards and Technology (NIST). I would offer that the cloud includes environments where physically distributed computing resources -- including infrastructure, applications, or databases -- connect in real time to help a company, consumer, or government agency perform a transaction, service, or inquiry.

Cloud services can be provided over the public Internet, but can also be done through connections over networks that run independently. Government agencies often establish clouds independent of the open Internet due to perceived risks of making data available over public channels -- but the government is moving in the direction of more use of the open Internet for cloud as well.

Indeed, whether consumers, companies, and governments realize it, they are already in the cloud all the time. Many popular email services, including Gmail, Hotmail and Yahoo, function over the distributed networks that constitute the cloud, and provide access to millions of people. Businesses and governments are increasingly using the cloud for email as well.

Benefits of the Cloud

Cloud computing is much in the news and lexicon these days. Questions about the cloud include: does cloud help end users, will cloud help businesses and federal agencies carry out their mission, and will cloud reduce costs? The answer to all of these questions is “yes”.

Moving to the cloud brings numerous demonstrable benefits:

- **Cost Saving.** Cloud computing allows customers to pay for just the computer resources that they use. They can avoid both a large initial upfront expenditure in hardware and software, and ongoing operating and maintenance expenses for their own IT. Resource usage can be monitored, controlled, and reported in a transparent way for both the provider and consumer of the cloud service. Indeed, a Brookings Institution study found that “... agencies generally saw between 25 and 50 percent savings in moving to the cloud”; this same report refers to other studies which claim savings from 39% to 99%.
(http://www.brookings.edu/~media/research/files/papers/2010/4/07%20cloud%20computing%20west/0407_cloud_computing_west)
- **Increased Effectiveness.** Network outages are an ongoing challenge for IT departments. Cloud computing can offer a higher level of service and reliability, reduce the harm that can come from network outages, and provide for a more immediate response to emergency situations by enabling real-time transfer of IT services to areas that are not affected by emergency.
- **Optimized Computing Usage.** IT service providers see cloud computing not only as a means to better serve their customers, but also to optimize data center usage. In many centers, only a small fraction of computing capacity is used at any time; the remaining capacity sits idle. Cloud enables flexible scaling across customers based on demand, which increases capacity and cost-effectiveness.
- **Energy and Environmental Improvements.** While most computers and servers are certified as energy efficient, cloud takes green computing one step further -- decreasing electricity use, slashing carbon emissions, and reducing IT costs through cost-effective use of computer and network infrastructure. Cloud also opens avenues for telecommuting (e.g., through internet-based email), which brings added environmental benefits.
- **Innovation and Transformation.** Cloud computing can help to spur innovation and transform operations. In the next several years, and the use of the cloud to pave the way for business model innovation is likely to increase significantly – innovation that includes entering new lines of business, reshaping an existing industry, or transitioning into a new business role.

In addition, and as has been noted by both the current and previous Federal Chief

Information Officers at the Office of Management and Budget (OMB), Federal computer users have lagged behind industry in IT productivity gains from IT, with outdated applications and burdensome rules governing acquisition and management of IT services. Movement to the cloud can fundamentally transform how federal agencies leverage IT, and to make federal workers far more effective in their use of IT.

The Federal government has, of course, already begun to realize the benefits of cloud computing. Examples include:

- the development and implementation of governmentwide and specific cloud strategies from OMB and agencies,
- the recent introduction of the General Services Agency (GSA) Federal Risk and Authorization Management Program (FedRAMP) program that fosters interoperability in cloud services across agencies. Indeed, other governments are studying FedRAMP's implementation closely to possibly emulate the model; and
- work by the National Institute of Standards and Technology (NIST) to clarify and guidance on the cloud.

Key Issues for Discussion

Today, I would like discuss three main challenges for government in order to realize the full benefits of the cloud:

- how to implement cloud efficiently,
- how best to address security in the cloud, and
- how to leverage the cloud's global model effectively.

Implementation

Key for success in any cloud implementation is a strategy to define how to increase efficiency, save costs, and improve performance of programs in the cloud. A small investment in upfront planning can pay large dividends in measured outcomes from any cloud migration. This is especially important because most entities do not build brand new computing environments where all activities operate in the cloud. Rather, they integrate cloud-based infrastructure, applications, and services into existing legacy environments, and must make choices as to what technologies, processes, and data should migrate to the cloud, over what period of time, and at what cost. To guide those choices, organizations need a sound up-front strategy that considers investments relative to resource availability and mission objectives.

The IBM Center for the Business of Government has produced a number of papers that address cloud implementation, especially in the Public Sector. For example:

- In a 2009 report for the Center, “Moving to the Cloud: An Introduction to Cloud Computing in Government,” David Wyld provides non-technical executives with a roadmap to understand key questions to ask as their organizations move to the cloud. He frames key challenges facing government leaders in the space, including scalability, security, open standards, procurement, and legal issues.
- In 2010, author Costas Panagopoulos wrote in our semi-annual journal, The Business of Government, about the lessons learned in cloud implementation by the Census Bureau (“Counting on the Cloud: Early Reflections on the Adoption of Cloud Computing by the U.S. Census Bureau”). He outlines key lessons that include the need to start early in cloud design, to partner with other adopters, and to correct problems as soon as they arise.
- Many perspectives on how best to implement cloud appear on our blog site, concentrated primarily in “Strategies to Cut Costs and Improve Performance”. (<http://www.businessofgovernment.org/blogs/cut-costs-and-improve-performance>)

In addition, much research and experience demonstrates that to maximize the cloud’s benefits, organizations must move aggressively to adopt more standardized offerings across organizations. That is, they must change current technology, procurement, and business processes to conform to best commercial practice, rather than modifying the cloud to fit existing organizational processes. Standardized offerings provide economies of scale and allow providers to automate processes that result in lower costs for users.

In addition, while savings can be achieved by migrating current applications, not all existing applications can run in a cloud efficiently. Organizations can collect data on how applications are being used to make informed decisions about which applications to migrate to the cloud, and in what order. This data can also help to sunset unneeded applications and optimize IT more efficiently and effectively.

Finally, cloud implementation can enable innovation. Developers who come together over cloud-based platforms that rely on open standards can share ideas and test approaches in ways that take advantage of the wisdom of many, rather than the few who work on a custom application.

Security

Relinquishing direct control of the IT infrastructure by adopting the cloud has raised perceived concerns about security risks. Cloud computing, however, can provide for an environment that is inherently superior for applying many critical security measures. By centralizing data storage and governance, clouds can actually provide better security at a lower cost than can traditional computing environments. Cloud environments can also provide differentiated levels of security, reflecting the fact that some data requires a great deal of protection while other data requires far less. Cloud providers can work with their

customers to deliver security efficiently and effectively based on different levels of risk -- security services can be built into the cloud up front to optimize protection at a given risk level.

Moreover, by facilitating uniform management practices across a distributed computing environment, cloud can improve certain key security practices, such as:

- **Detection** - the cloud creates the ability to link together millions of security nodes on the net. By working together, these nodes can better detect new threats how to implement cloud efficiently.
- **Remediation** - Quick remediation is vital for cyber security - the less time the malware is present, the better the protection. The cloud allows implementation much more rapidly than the older model of having to load the solution onto multiple machines.
- **Prediction** – Increasingly, cyber security focuses on limiting the ability of bad actors to act in the first place. The cloud helps security teams to identify machines that create and disseminate malware, and to quickly isolate those machines – blocking their ability to infect customer systems.
- **Data and Device Protection** – A significant security threat, and one that has impacted the Federal government, is breach of data, especially from lost or stolen laptops or mobile devices. Cloud provides for centrally stored data with continuous and automated network analysis and protection, so that if a device is lost, the data and applications are not lost with it (unless the user has been allowed to load them separately onto the device).

As noted earlier, I also Chair the Federal Information Security and Privacy Advisory Board (ISPAB). Building off a Board-hosted forum on best practices in this space several years ago, the ISPAB has highlighted numerous ways that the Federal government can best address security in the cloud, especially with regard to the operation of the FedRAMP program and the monitoring of traffic that flows in and out of agencies over cloud-based applications (see more at <http://csrc.nist.gov/groups/SMA/ispab>).

Global Model

The cloud can be either localized or global in nature. The benefits of cloud computing increase, however, when providers can move computing and data power to locations that are most cost-effective, rapidly and with no loss of service quality or security. For example, consider the recent storm and power outages in Washington, DC -- in a situation like this, using a cloud that allows the online relocation of computing resources would provide continuity of service far more quickly and cheaply than a platform restricted to local computing locations.

Real-time movement of computing resources points out the need to understand issues

involved in cross-border data flows in the cloud. Of course, data has moved across borders for decades -- airlines, pharmaceuticals, telecommunications, and technology companies are among those with long history here. The cloud has amplified attention to cross-border data flow issues such data sovereignty and jurisdictional questions. Most of these issues are best addressed via contracts between solution providers and customers; contracts can designate jurisdiction and establish clear provisions for ownership, privacy, security, and consumer protection.

I would like to highlight some recent findings and observations in three areas that affect the cloud's global nature and American competitiveness in this space – the extent that government can access data across borders, international privacy collaboration, and open standards.

Government Access to Data

The extent to which governments can access data across borders is a subject of confusion among cloud providers and users. However, many nations have similar domestic data policies. A recent HoganLovells White Paper, “A Global Reality: Governmental Access to Data in the Cloud,” reveals that U.S. law provides some greater privacy protections:

“In jurisdictions outside the United States, there is the real potential of data relating to a person, but not technically “personal data,” stored in the Cloud being disclosed to governmental authorities voluntarily, without legal process and protections. In other words, governmental authorities can use their “influence” with Cloud service providers – who, it can be assumed, will be incentivized to cooperate since it is a governmental authority asking – to hand over information outside of any legal framework. United States law specifically protects such data from access by the government outside of legal process.”

Furthermore, the paper notes that “it is not possible to isolate data in the Cloud from governmental access based on the physical location of the Cloud service provider or its facilities. Governmental access to data in the Cloud is ubiquitous, and extends across borders.” As the paper concludes, a detailed analysis of ten countries revealed that:

“every single country that we examined vests authority in the government to require a Cloud service provider to disclose customer data in certain situations, and in most instances this authority enables the government to access data physically stored outside the country's borders, provided there is some jurisdictional hook, such as the presence of a business within the country's borders. Even without that “hook,” MLATs allow access to data across borders.” [Governments cooperate with each other through “mutual legal assistance treaties” (MLATs)]

Regardless of jurisdiction, individuals whose data resides in the cloud will have greatest confidence if, to the extent permissible under law, they do not lose protection solely based on where their data is stored and processed.

International Privacy Collaboration

With the understanding that many nations have similar laws and that where a company stores its data should not reduce protections, consumers, enterprises, and governments can look at cloud providers' experience with providing security and privacy protections in order to make informed decisions about how to use applications in the cloud.

In addition, cloud computing would benefit from an international regime that promotes privacy while supporting the efficient flow of data across borders. While it is neither practical nor desirable to seek the complete harmonization of rules, countries may be able to recognize each other's rules (including privacy safeguards) to the greatest extent possible, and to honor those rules through means such as contracts and service level agreements (SLAs). This approach to interoperability would not require the same laws in each jurisdiction, but it would allow data and computing transfers to take place over the cloud based on shared understanding of how law and policy should apply.

Initiatives such as the US-EU safe harbor, the use of binding corporate rules, and the cross-border privacy initiative in APEC serve as building blocks for such an interoperable international privacy regime. The benefits of such a regime would extend beyond cloud computing; they would support any entity that builds data centers in different jurisdictions. But because cloud computing relies heavily on the efficiencies gained from real-time data flows across different countries, the adoption of an interoperable privacy regime would facilitate cost-effective adoption.

Open Standards

The benefits of cloud can best be achieved by reliance on open standards that promote data portability and interoperability, which are critical for successful adoption and delivery of cloud-based solutions. Open standards enable users to reap value from a diversity of cloud providers, and to move data and applications based on a choice of available applications without friction. Consider the analogy to Internet-based computing since the 1990s: the Internet has seen phenomenal growth and spurred so much innovation because its networks dependent largely on open standards -- no one company or handful of companies has a dominant position and can single-handedly determine its architecture and development.

An open standards approach would particularly help to address the issue of location-based mandates. Over a dozen countries have recently drafted or are considering laws that would mandate in-country location of cloud data servers and storage facilities. The Business Roundtable recently released a report, "The Growing Threat of Local Data Server Requirements" (http://businessroundtable.org/uploads/studies-reports/downloads/Global_IT_Policy_Paper_final.pdf), which provides details on this issue. While certain practices by governments to locally source cloud computing are understandable – for example, for a country's national security information – governments could enhance the cloud's efficiency and cost benefits by avoiding location

mandates, and leveraging and encouraging an open, global model.

Conclusion

Cloud computing has great promise to enable consumers, businesses, and governments to reduce IT costs and improve IT performance. Key considerations in leveraging the benefits of the cloud include implementation, security, and leveraging the efficiencies of the global model. Greater education, investment and appropriate incentives can allow government and businesses to help all stakeholders use the cloud most effectively.

Chairman Goodlatte and Ranking Member Watt, thank you for the opportunity to speak with the Subcommittee. I welcome the chance to answer any questions that you may have.