SIIA WHITE PAPER

Guide to Cloud Computing for Policymakers

CLOUD COMPUTING

Software & Information Industry Association
www.siia.net

DEVELOPED BY THE PUBLIC POLICY DIVISION OF THE
SOFTWARE & INFORMATION INDUSTRY ASSOCIATION (SIIA)

Guide to Cloud Computing for Policymakers

SIIA is the principal trade association of the software and digital information content industries. SIIA provides global services in public policy, business development, corporate education and intellectual property protection to the leading companies that are setting the pace for the digital age. SIIA has played a pivotal role in the development and legitimization of the Software as a Service (SaaS) and Cloud Computing models. Reaching back to 1999, SIIA began identifying the standards, best practices and business models for SaaS that are now commonplace in cloud computing. Many of our member-companies, both large and small, are key enablers of cloud computing.

I. Introduction

The Software & Information Industry Association (SIIA) produced this paper as a guide to cloud computing for policymakers. It explains that cloud computing is not a new, nor singular technology, but rather an evolving mechanism for IT consumption and delivery, provisioning a wide variety of computing services from remote locations. The technology has been part of the computing landscape for decades, but with the widespread deployment of broadband communications facilities, it is increasingly within the reach of businesses and individual customers.

From our work with policymakers, SIIA understands that they are interested in fostering the growth of cloud computing to seize the economic benefits and protect their citizens against any potential harm. Yet, because cloud computing is not a single technology or business model, for policy making purposes, there is no such thing as "the cloud." **The basic conclusion of this paper is that, to provide for the safe and rapid growth of cloud computing, there is no need for cloud-specific legislation or regulations, and in fact, such actions could impede the potential of cloud computing.**

There are currently a number of existing and proposed policies that could hurt the development of cloud computing. These include such things as requirements for the location of computer facilities in particular jurisdictions or restrictions of cross-border data flows. This paper concludes that policymakers should take great effort to remove or avoid such types of policies. Policymakers should instead join with industry and civil society to foster industry best practices and see that they are properly enforced.

In this paper, SIIA includes a section that addresses how best to accomplish public policy objectives, such as the provision of adequate privacy and security in the cloud, and we outline recommendations for policymakers. We have also prepared a fact sheet that highlights and debunks many of the most common myths that threaten the benefits of cloud computing.

This paper also addresses the different technologies, platforms and service models that comprise cloud computing, highlighting how this complexity makes defining cloud computing impractical for policy purposes. The paper then discusses the vast transformative benefits of cloud computing. However, the paper does not suggest that cloud computing is the sole, or even the most appropriate, answer for all enterprises or customers—rather, that it should be one option among others for IT customers.

II. Executive Summary

Cloud computing is not a new, nor singular technology, but rather an evolving IT consumption and delivery mechanism, provisioning a wide variety of computing services from remote locations. It is an evolution of IT architecture from centralized computing to network dependent systems with distributed assets and distributed management responsibilities. The technology has been part of the computing landscape for decades, but with the widespread deployment of broadband communications facilities, it is increasingly within the reach of businesses and individual customers.

While there are common definitions, the various different technologies, platforms and service models that comprise cloud computing reveal its complexity, and that defining cloud computing is impractical for policy purposes. Regardless of the challenges to define what is, or is not, "cloud computing," or the myriad platforms and service models that comprise it, cloud computing provides substantial benefits that are driving rapid adoption, including: on demand access, resource pooling, flexibility and elasticity, rapid implementation and energy efficiency, among others.

Transformative Benefits of Cloud Computing

Increased adoption by organizations of all sizes around the world—both private sector and governments—has clearly demonstrated that cloud computing offers three transformative benefits. Policymakers should consider these as they seek to ensure the efficiencies and economic benefits of cloud computing.

Economic Growth:
Cloud computing provides a strong engine for growth across businesses and regions.

While the growth of the cloud computing industry is strong, even more important is the effect cloud computing will have as an engine for driving growth across other sectors—growth made possible by greater access to advanced computing resources, often at lower prices. Cloud computing provides an IT environment where technology can be located in accordance with infrastructure and labor efficiencies, rather than being localized and provisioned independently, capitalizing on the economies of scale of network computing like never before.

As a result, cloud computing presents a major innovative opportunity to businesses of all sizes, and across all sectors of the economy. This opportunity is especially critical for the opportunities provided to small and medium-sized entities (SMEs) that lack the ability to make substantial investments in local IT resources. With cloud computing, SMEs can innovate more effectively and grow more quickly, therefore leveling the playing field.

Not only is this benefit significant to businesses, it will also have a transformative effect on governments, especially in regions where access to necessary technological infrastructure is limited. Countries that face shortages of trained IT professionals stand to benefit tremendously from cloud computing, provided they have adequate connectivity. With cloud computing and an internet connection, researchers, government employees, and entrepreneurs anywhere have access to the same quality of software applications.

Accordingly, it can be expected that the macroeconomic impact of the cloud is similarly large. Recent research has indicated that cloud computing can promote economic growth and competition, and it can help encourage broader economic recovery from the current downturn.

More Choice, Lower Cost:
As reliance on open standards and software and data interoperability are maximized, cloud computing can lead to greater choice and lower prices for consumers.

The movement towards cloud computing has increased the need for open standards for software and data interoperability. Open standards are critical for the successful adoption and delivery of cloud computing, which requires an environment where services can be provisioned efficiently and effectively across multiple browsers, and can run on multiple platforms such as desktop personal computers, and myriad mobile devices. There is a great promise for dramatically increasing competition among providers of computing technologies and ending the era of vendor lock-in. Over time, this will lead directly to greater choice and lower prices for consumers.

To achieve this vision, the cloud computing industry needs the flexibility to experiment to reach the most efficient and innovation-promoting degree of open standards IT architecture. To that end, the current collaborative government-industry cooperation across various forums to accelerate the standards and reference architecture development process is very promising for the mutual goal of advancing the rapid adoption and long-term effectiveness of cloud computing.

Better Security:
Cloud computing provides an environment inherently superior for applying many critical security measures.

As complex networked systems, “clouds” are affected by traditional computer and network security issues such as the need to provide data confidentiality and maintain data integrity and system availability. While the cultural change of relinquishing direct control of the IT infrastructure has created fear for some IT professionals, there is a much less recognized reality that cloud computing, by nature, provides an environment inherently superior for applying many critical security measures.

By enabling uniform security management practices, clouds are capable of improving on several key security practices, such as predicting and detecting new threats, providing for quicker remediation, and providing for greater protection against end user breach or corruption, and lost or stolen data.

Policy Implications & Recommendations

Policymakers are rightly interested in fostering the growth of cloud computing to seize the economic benefits, and to protect their citizens against any potential for harm. Yet, because cloud computing is not a single technology or business model, for policy making purposes, there is no such thing as "the cloud." **The basic conclusion of this white paper is that there is no need for cloud-specific legislation or regulations to provide for the safe and rapid growth of cloud computing, and in fact, such actions could impede the great potential of cloud computing.**

Today, there are a number of existing and proposed public policies that could hurt the development of cloud computing, such as requirements for the location of computer facilities in particular jurisdictions, or restrictions of cross-border data flows—policymakers should take great effort to remove or avoid such types of policies.

With the goal of helping policymakers foster the effective development and adoption of cloud computing, while at the same time ensuring that users are served effectively, this paper examines the following key policy areas: Privacy, Security, Open Standards, Jurisdiction, Localization Rules and Cross-Border Data Flows, and it concludes that one-size-fits-all policies cannot apply properly to all the various technologies and business models that comprise cloud computing.

Policymaker concerns about specific issues can and are being addressed through industry-led voluntary action, public-private partnerships and best practices enforced through contracts and existing legislation. SIIA recommends that policymakers embrace the following key principles in their efforts to develop policies that encourage the economic benefits of cloud computing and ensure that users are protected:

- Avoid cloud-specific rules and policies, in favor of policies that apply broadly to a wide range of technologies and services, and those that maintain a level playing field for cloud computing and all approaches to remote computing and data storage.
- Promote open standards for software and data interoperability, and avoid policies that would favor one particular business model or technology over another.
- Promote policies that allow to the greatest extent possible, unrestricted transfer of data across borders.
- Encourage rules governing data to travel with the data in order to adequately recognize varying jurisdictional requirements, and ensure data subjects do not lose protection when their data is stored and processed in "the cloud", or in any remote computing environment.
- Avoid localization mandates, or any policies that would give preference to data processors using only local facilities or operating locally.

- Seek interoperable privacy regimes in which countries recognize each other's privacy rules to the greatest extent possible.
- Embrace a global approach to cybersecurity that recognizes the global nature of interconnected systems and provides for data to be protected regardless of where it is located, and that seeks international consensus standards that avoid fragmented, unpredictable national requirements.

III. Defining the Core Attributes and Benefits Of Cloud Computing

Cloud computing represents a natural evolution of information technology (IT) architecture from centralized computing to network dependent systems with distributed assets and distributed management responsibilities. Rather than being a new technology, cloud computing is a new way of delivering and consuming computing resources, ranging from the simple provision of IT infrastructure and software, to a platform comprised of a combination of various technologies together, accessed remotely via the Internet.

This is why efforts to define cloud computing are continually challenging. As defined by the U.S. National Institute of Standards and Technology (NIST), cloud computing is "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." NIST has identified five essential characteristics of cloud computing: (1) on-demand service, (2) broad network access, (3) resource pooling, (4) rapid elasticity, and (5) measured service.[1]

This is a very sound description, broadly recognized as the core definition of cloud computing. However, a deeper look at the definition reveals that the term "cloud computing" is an even broader concept, referring to a combination of various complex technologies, such as computers, programming languages and software programs, that when provided in various approaches, have few core characteristics in common.

For instance, beyond the base definition above, NIST goes on to explain that cloud computing consists of three service models, which can be offered across three different deployment models. The service models consist of Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS):

> SaaS consists of firms offering the capability to use software applications that are housed off the user's premises. Examples are the customer relationship management tools that Salesforce.com provides and the office productivity suites available from Google. These services are a natural outgrowth of the software programs that have been resident on and used in stand alone computing environments.
>
> PaaS services allow users to develop their own Web-based applications or to customize existing applications using one or more programming languages and development tools. Examples include Amazon's Elastic Compute Cloud and Google's App engine. These services are natural extensions of individual computer platforms like Linux and Windows.
>
> IaaS services allow customers to access the equipment and hardware needed to perform computing operations, including storage, processing and networking components. Examples include Amazon's Web Service or Red Hat's CloudForms.

The three deployment models through which these services can be provided, separately or together, are: (1) private clouds, (2) public or 'community' clouds, or (3) hybrid structures. Private clouds are exclusive to a single user. Public or community clouds are available to the general public or shared by large diverse groups of customers, and hybrid clouds combine public and private elements in the same data center.

In addition to the variety of technologies encompassed by the term "cloud computing," different business models are involved. The most basic distinction is between services that are offered to the general public and those that are provided to business customers. Amazon's music in the cloud service allows individuals to store their music in remote facilities and access it through a variety of devices. Yahoo and Google provide email services to the general public that can be accessed from any personal computer or mobile device. In contrast, IBM and Oracle offer a variety of cloud computing services to large enterprise customers. Amazon and Google services target small and medium-sized enterprises and start ups.

The policy issues that arise in the context of business-to-business transactions are entirely different from the issues that arise in the context of transactions with the general public. Yet the term "cloud computing" applies to both business models.

Because of these varying models and platforms, and contrary to the common term, "cloud computing" resists practical definition for common treatment by law and regulation. Simply stated, cloud computing is not a single, unitary thing. There is no "the cloud."

The evolution of IT architecture from centralized computing to network dependent systems with distributed assets and distributed management responsibilities provides substantial benefits not previously available to many customers. This is true regardless of the challenges to define what is, or is not, "cloud computing," or the myriad platforms and service models that comprise it. Although cloud computing is not always the best fit for all customers, the following core benefits are driving rapid adoption and will continue to do so for the foreseeable future:

- **Increased, on Demand Access.** Computing capabilities are accessible through standard devices using thin or thick client platforms such as a simple browser in a mobile phone, tablet or laptop. A consumer can unilaterally provision computing capabilities, such as server time and network storage as needed.
- **Resource Pooling.** Computing resources can be pooled to serve multiple consumers with resources dynamically assigned and reassigned according to consumer demand.
- **Flexibility and Elasticity.** IT departments that anticipate fluctuations in user load do not have to scramble to secure additional hardware and software. They can add and subtract capacity as the network's load dictates.

- **Cost Savings.** In addition to enabling customers to avoid the large initial upfront expenditure in hardware, software and development tools, resource usage can be monitored, controlled, and reported; providing transparency for both the provider and consumer of the utilized service, and allowing customers to pay only for the computer resources that they use.
- **Increased Effectiveness.** Users, particularly individuals and small and medium-sized IT departments, can often benefit from a higher level of service and reliability, reduced threat of network outages and a more immediate response to emergency situations.
- **Rapid Implementation.** Projects can often be launched more quickly as a result of more flexible procurement and certification processes, and an increasing selection of services, tools, and features.
- **Energy Efficiency.** Resource pooling eliminates the need for each user community to have its own dedicated IT infrastructure, so multiple users can share computing resources, leading to higher utilization rates, fewer servers, and less energy consumption.
- **Enhanced Security Capability.** By enabling uniform security management practices, clouds are capable of improving on certain key security practices, such as improved prediction, detection and remediation of threats, as well as the ability to provide better protection against end-user breach and corruption.

IV. Transformative Benefits of Cloud Computing

There is an adage in technology that while we tend to overestimate the short-term impact, we also tend to underestimate the impact over the long term. This is most certainly true with cloud computing. While the recent progress is worth of all the attention cloud computing has received over the last 3-5 years, we are still in the beginning phase of more than a decade-long journey. The goal is to achieve an IT environment that has widespread benefits for not just consumers, but also businesses and nations around the world.

While it is impossible to predict with great clarity the long-term impact of cloud computing, increased adoption by organizations of all sizes around the world—both private sector and governments—have clearly demonstrated that there are three transformative benefits of cloud computing. This section provides an analysis of the following three game-changers, with the goal of helping inform policymakers decisions as they seek to increase the efficiencies and the social and economic benefits of cloud computing:

- **Economic Growth:**
  Cloud computing provides a strong engine for growth across businesses and regions.
- **More Choice, Lower Cost:**
  As reliance on open standards and software and data interoperability are maximized, cloud computing can lead to greater choice and lower prices for consumers.
- **Better Security:**
  Cloud computing provides an environment inherently superior for applying many critical security measures.

Economic Growth: Cloud computing provides a strong engine for growth across businesses and regions.

Research indicates that the cloud computing industry segment is substantial and growing. According to recent research by Gartner, cloud services revenue was projected at approximately $68.3 billion in 2010, and the industry is poised for strong growth through 2014, when world-wide cloud services revenue is projected to reach $148.8 billion.[2]

While the growth of the cloud computing industry is strong, even more important is the effect cloud computing will have as an engine for driving growth across other sectors—growth made possible by greater access to advanced computing resources, often at lower prices.

Cloud computing creates efficiencies for individuals and enterprises that no longer have to purchase and maintain their own computing resources, and the great potential for cost savings that go along with this on-demand approach. This efficiency derives from the fundamental nature of cloud computing that builds on the framework of the internet and further breaks down borders. This ability to foster a seamless flow of information and IT resources where technology can be located in accordance with infrastructure and labor efficiencies, rather than being localized and provisioned independently, capitalizes on the economies of scale of network computing like never before.

Cloud computing provides elasticity, enabling customers to leverage the shared underlying capacity of IT resources via a network. Customers can quickly request, receive, and release resources as needed. As a result of this elasticity, customers can avoid the risk of over-provisioning resources to build for capacity demand. Therefore, they can pay for only what they need, when they need it, and resources needed to support mission critical capabilities can be provisioned more rapidly and with minimal overhead and routine provider interaction. Accordingly, "unused" resources can be redeployed to other business imperatives.

In many cases, cloud computing is provided via a convenient rental of computing resources: users pay service charges while using a service but need not pay large up-front acquisition costs to build a computing infrastructure. The reduction of up-front costs reduces the risks for pilot projects and experimental efforts, which supports organizational flexibility.

As a result, cloud computing presents a major innovative opportunity to businesses of all sizes, and across all sectors of the economy. This opportunity is especially critical for the opportunities provided to small and medium-sized entities (SMEs) and underserved regions that lack substantial investment in local IT resources. SMEs can innovate more effectively and grow more quickly. Therefore, cloud computing levels the playing field by enabling start-ups and smaller businesses to compete more effectively with larger companies.

Recent research has indicated that these fundamental characteristics of cloud computing can promote economic growth and competition, and it can help encourage broader economic recovery from a severe downturn like the current one.[3] Today, one of the greatest barriers to growth for SMEs is the massive up-front investment required for IT infrastructure.

Cloud platforms and new data centers are creating a new level of infrastructures that can be exploited by businesses, to the greatest benefit of SMEs, and help to free-up new investment and business opportunities at a time when growth is critical.

Beyond the reduction of the fixed costs of entry and production, other key cloud attributes such as the ability to more rapidly modify and customize software applications to meet the needs of niche business models and the ability to share computing resources by a large pool of users, are combining to create an environment where growth of businesses, particularly SMEs, is enabled to an extent not seen since the introduction of the Internet in the 1990s, and perhaps even greater. Accordingly, it can be expected that the macroeconomic impact is similarly large.[4]

Not only is this benefit significant to businesses, it will also have a transformative effect on governments around the world, especially in regions where access to necessary technological infrastructure is that much harder. Countries that face shortages of IT professionals trained on the latest computing technologies stand to benefit tremendously from cloud computing, provided they have adequate connectivity. With cloud computing and an internet connection, researchers, government employees, and entrepreneurs in any country can access the same quality of software applications.[5]

More Choice, Lower Cost: As reliance on open standards and software and data interoperability are maximized, cloud computing can lead to greater choice and lower prices for consumers.

The movement towards cloud computing has increased the need for open standards for software and data interoperability. That is, consumers of cloud computing recognize the great promise for dramatically increasing competition among providers of computing technologies and ending the era of vendor lock-in. Over time, this will lead directly to greater choice and lower prices for consumers.

The reason the internet saw such phenomenal growth and spurred so much innovation in the late 1980s and 1990s is because it was a "network of networks." An open framework built on the backbone of open standards like HTML and TCP/IP, the internet has enabled myriad entities and individuals to build and run their piece of the network infrastructure. Additionally, no one company or handful of companies has been able to establish a dominant position and determine the standards or architecture of the network or the internet. Rather, the internet has flourished as the single greatest network dependent largely on open IT standards.

In many ways, cloud computing is an extension of internet-based computing. Therefore, continued reliance on open standards is critical for the successful adoption and delivery of cloud computing, both within the public sector and more broadly. Open standards encourage competition by making data and applications usable and re-usable across providers, allowing users to shift services between providers and take advantage of cost savings or innovative new product functionality. Entrepreneurs thrive in community environments knowing their innovations will work across applications, platforms and networks. Open standards ensure that all interested parties can make, use and re-use data and contribute with innovative applications to generate added value to benefit consumers and societies, as well as to spur innovation and economic growth.

An ICT environment based on open IT standards is critical to spur interoperability and realize the ideal vision of cloud computing—a vision where users have the opportunity to benefit from greater choice and lower costs. Such an environment is one where cloud services can be provisioned efficiently and effectively across multiple browsers, and can run on multiple platforms such as desktop personal computers, and myriad mobile devices such as tablets and mobile phones.

While there should continue to be a wide range of programming languages, cloud platforms and service configurations should provide for greater advancement of those that are based on open standards and easily implemented across myriad applications. In this environment, cloud providers will be able to enhance interoperability through the use of open, documented application programming interfaces (APIs), provide access to their data in open standard formats to which users have reasonable access—including reasonable license terms—to provide for users to not only access and retrieve their data, but also to return it to local storage or transfer it to another cloud provider if desired.

Today, there are multiple private sector led efforts to help advance standards for cloud computing to achieve this interoperable vision for cloud computing. Having already helped establish broadly adopted definitions for the three commonly recognized cloud deployment models (i.e., public, private and hybrid) and three service models (i.e., Infrastructure as a Service, Platform as a Service, and Software as a Service), the United State's government, through NIST, is currently playing a leadership role in prioritizing, developing, evolving and refining standards over time. This role is critical as the collective requirements for standards evolve in response to operationally driven innovation and technology evolution. Specifically, the effort is focused on accelerating cloud standards for software and data interoperability, including helping to define the standards, and collaborating with government IT professionals, private sector experts, and international bodies to identify, prioritize, and reach consensus on standardization priorities.

The cloud computing industry needs the flexibility to experiment to reach the most efficient and innovation-promoting degree of open standards IT architecture. To that end, the current collaborative government-industry cooperation across various forums to accelerate the standards and reference architecture development process is very promising for the mutual goal of advancing the rapid adoption and long-term effectiveness of cloud computing.[6]

Better Security:
Cloud computing provides an environment inherently superior for applying many critical security measures.

Security in an IT architecture is very much an exercise in risk management. Risk management entails identifying and assessing risk, and taking the steps to reduce it to an acceptable level. Throughout the system lifecycle, identified risks must be carefully balanced against the security and privacy controls available and the expected benefits. Too many controls can be inefficient and ineffective. As with any technology, it is critical to strike the appropriate balance between the number and strength of controls, and the risks associated with the technological solutions.

As complex networked systems, "clouds" are affected by traditional computer and network security issues such as the need to provide data confidentiality and maintain data integrity and system availability. While there is some fear of greater risks with cloud computing because of the cultural change of relinquishing direct control of the IT infrastructure, there is a much less recognized reality that cloud computing, by nature, provides for an environment inherently superior for applying many critical security measures. By enabling uniform security management practices, clouds are capable of improving on certain key security practices, such as:

- **Detection** - Cloud computing creates the ability to link together millions of security nodes on the net. By working together, these nodes can better detect new threats.
- **Remediation** - Quick remediation is a critical component of cybersecurity - the less time the malware is in the system, the better protected you are. Cloud computing allows security providers to implement the solution much more rapidly than the traditional model of loading the solution onto multiple machines.
- **Prediction** - One of the most effective strategies for cybersecurity is to limit the ability of bad actors to act at all. Cloud computing allows solutions providers to build reputation scores of machines that are bad actors, creators and disseminators of malware. The cloud solution can enable the provider to build reputation scores, much like credit scores, and block the ability of bad actors and bad machines to infect customer systems.
- **Protection against end user breach or corruption** - One of the greatest threats to security derives from the user side, in the form of data breach or corruption resulting form lost or stolen laptops, mobile devices and portable drives. Cloud computing can eliminate or minimize these threats through the use of centrally stored data with continuous and automated network analysis and protection.

V. Policy Implications / Recommendations

Many policymakers have expressed a strong interest in fostering the effective development and adoption of cloud computing, while at the same time ensuring that users are served effectively. This section addresses those objectives, examining the following key policy areas:

- Privacy
- Security
- Open standards
- Jurisdiction
- Localization Rules
- Cross-Border Data Flows

Before exploring these key topics, however, one general overarching point needs to be made: **Cloud specific legislation or policies are counterproductive.**

As described above, the term cloud computing covers a variety of technologies and business models. It has aspects of hardware, programming languages, platforms, software applications and networking. It includes services provided to the general public and to other businesses. It covers both business-to-business service and the businesses that are built on top of cloud services and offered to the general public. No single one-size-fits-all policy could apply properly to all these technologies and business models. For instance, a rule that makes sense when applied in a business-to-consumer context might be inappropriate when applied in a business-to-business context. In addition, a rule that might apply to a public cloud offering might not work as applied to a private cloud offering.

Accordingly, there is no need to craft cloud-specific legislation or regulations. As the following discussion suggests, policymaker concerns about specific issues can and are being addressed through industry-led voluntary action, public private partnerships and best practices enforced through contracts and existing legislation. The remainder of this section examines specific policy issues with this perspective in mind.

Privacy

It is important to explore what the appropriate privacy rules for cloud computing should be. This section makes two points. First, cloud computing is not a "sector" like financial services or healthcare that needs sector-specific privacy rules. Second, cloud computing would benefit from privacy regimes that interoperate, that is, that allow data to flow back and forth in a seamless fashion from computers located in different jurisdictions.

In a business-to-business context, cloud computing firms provide services to businesses in particular sectors such as energy, financial service, telecommunications, health care and a wide range of others. In a sectoral regime such as in the United States (US), these businesses are sometimes subject to existing privacy legislation and rules. For instance, the Graham-Leach-Bliley Act (GLBA) covers financial services and the Health Insurance Portability and Accountability Act (HIPAA) for healthcare providers.

Under GLBA, for example, financial service companies are not permitted to share data with third parties for marketing purposes without customer consent. If financial services companies provide computing services to themselves through in-house IT departments and leased or customized software applications, they must design their systems to meet this and other privacy obligations. If they obtain computing services through an outsourcing arrangement with a cloud computing provider, they still must satisfy their privacy obligations and typically require the cloud provider to provide services that satisfy these obligations as part of their contract. There is no need for special privacy rules that apply to the cloud provider because privacy protections are gained through whatever obligations fall on the entity that has collected the data.

In other regimes such as the European Union (EU), special obligations fall on outside data processors. If a non-EU-based company operates a data center for a particular company, they would be subject directly to the EU's Data Protection Directive. Such obligations would also apply to cloud providers that might provide a public cloud for the general public.

Because cloud computing presents only a new method of storage, consumption and delivery of traditional IT services, it is not a unique context or sector for which a unique privacy regime would be effective. In most cases, the rules for cloud computing follow the rules for the context in which it is operating, which should not be dealt with separately from the application of privacy rules applied in any traditional context.

Cloud computing would benefit from an international privacy regime that allows for data transfers across borders. It is not practical to seek the complete harmonization of privacy rules, but it is practical for countries to recognize each other's privacy rules to the greatest extent possible, and to honor those rules through contacts and service level agreements (SLAs).

Initiatives such as US-EU safe harbor, the use of binding corporate rules and the cross-border privacy initiative in APEC would build such an interoperable international privacy regime. The benefits of such a regime extend beyond cloud computing. They would benefit a company that builds its own data centers in different jurisdictions. Since cloud computing relies heavily on the efficiencies gained from localizing services in different jurisdictions, it would benefit from the adoption of such an interoperable privacy regime.

Security

Cloud computing provides an environment that in many ways is inherently superior for applying various critical security measures. By centralizing data storage and governance, it can provide better security at a lower cost than trying to protect data in many dispersed locations. Still, some types of cloud offerings present special challenges, and some policy makers are exploring whether special security requirements for cloud computing are necessary.

Similar to the privacy space, government mandated cloud-specific security rules are not necessary. The security requirements for many cloud computing offerings are not different from the security requirements for in-house storage of data or for security at an off-premises data center. Where data and applications from many customers are housed in the same facilities, and in many cases on the same servers, there need to be special technical and administrative measure taken to prevent unauthorized access to customer data. This fact is well understood by the industry, and best practices are evolving to respond to the challenge.

In other areas, such as the payment card industry, the industry itself responded by autonomously developing security standards that reflected the unique challenges of the context. For example, the Payment Card Industry Data Security Standard was developed by the payment card brands to promote good security among banks, processors and merchants who handle card holder data. It contained very specific rules such as not storing security codes that were designed to prevent hackers from gaining access to information that could be used to make counterfeit cards. Governments did not develop or require the development of this standard, and governments need not develop a specific set of security requirements for cloud computing environments.

Some firms are subject to special regulations with respect to security. In the United States, special security rules apply to financial service providers under the Gramm-Leach-Bliley Act (GLBA). In addition, some firms face obligations under the Federal Trade Commission's decisions to provide reasonable security. Security rules apply across all sectors under the generic data protection regimes in force in many jurisdictions including the European Union.

In a business-to-business context, these rules have to be accommodated by the cloud computing provider as part of the service provided to each customer. If new security rules are needed for critical infrastructure as part of a national effort to protect a country against cyber attacks, those rules should apply to an IT provider that is providing a service that is covered critical infrastructure, whether provisioned as "cloud computing" or as another IT infrastructure.

There might be good reasons to have security rules, either for specific sectors or generic rules that apply across the board to all businesses that store or process information. There is no reason to develop security rules specific to cloud computing providers that differ from other methods of provisioning similar IT services. That is, following a technologically neutral approach, government security requirements should apply evenly to IT services provided either via a cloud platform, or traditional client-server offerings that have been widely utilized for many years.

Further, cybersecurity goals should be applied from a global perspective. Enactment of new national requirements—without taking into consideration the global nature of interconnected systems—would be counterproductive because these requirements would increase costs and prevent the development of measures that can protect data no matter where it is stored. Cyber threats are global and the practices that respond to them must be global as well. Policymakers should avoid fragmented and unpredictable rules in the international sphere that frustrate innovation, seamless flow of information, and the broad commercial success of the online environment.

Open Standards

The previous sections also explain the importance of an open standards-based cloud infrastructure, where opportunities for software and data interoperability are maximized by open standards. Whether using a cloud or "traditional" IT environment, customers should be able to seamlessly—and in real-time— move their data and maintain a choice of various available applications to work with. This interoperability requirement is even more important in cloud computing, as it is critical to fulfilling expectations of increased choice among customers—including businesses, governments and individual cloud users.

The government has a key role in this area as a facilitator and convener of private standards groups. Industry-led standards development organizations are best equipped to determine which technical standards will best implement the policy goal of interoperability. Government can encourage, push, facilitate and cajole, but it should not take over the process by imposing its own views of the best technical standards, or trying to create new standards where they may not yet exist.

In addition, governments should avoid mandating business models under the guise of promoting "open standards," or establishing rules that dictate to the use of applications that interoperate with applications provided by other cloud computing providers or establishing data interoperability to their customers. The forces of competition are strong in this area, so any company that tries to lock in its customers through overly narrow choices of storage formats, programming languages and platforms and software applications will not gain or retain customers.

Attempts to dictate interoperability conditions would have the undesirable consequence of reducing the marketplace to a standardized set of products and services—plain vanilla cloud computing services. The advantages of innovation will be lost if all applications have to be standardized in this fashion and the only thing left to compete on is price.

Jurisdiction

Cloud computing providers face the need to apply local law to transactions that cross borders. But cloud computing is not unique in this regard. Since the beginning of electronic commerce, governments, private industry and civil society groups have tried to sort out the right way to proceed in the face of the split jurisdiction that applies to cross-border transactions. Cloud solutions could add some complexities, as the number of countries that might legitimately claim jurisdiction over the data could increase. One key challenge is the determination of whether the law of the buyer or seller applies. Another is whether the jurisdiction of the data subject prevails over the jurisdiction where the data is stored or processed. The legal regimes at issue include privacy, security, and consumer protection.

Most often, these issues are properly addressed via contracts between solution providers and customers. Contracts have--and will continue to--adequately identified which jurisdictions should prevail, therefore establishing responsibilities for setting and managing appropriate privacy, security and consumer protection procedures.

Data subjects should not lose protection when their data is stored and processed in the cloud, or in any remote computing environment. Meaning, the rules governing data should travel with the data. For example, US financial services regulators have adopted this perspective with respect to processing of data by service companies serving financial institutions. The privacy and security rules that apply to data if stored and processed in-house apply if the data is stored and processed by an external service provider, even if the external service provider is located in another country.

This approach provides a practical starting point, even if not fully solving all of the complex questions that may arise as data is inevitably more subject to multiple jurisdictions. Longer term, the best way to resolve conflicts of jurisdiction is to strive for an international accommodation in which regimes recognize and accept each other's legal structures. This ideal of interoperability would not require the same laws in each jurisdiction, but it would allow transfers to take place without being blocked by the differences.

Localization Rules

Localization rules, those that require providers of computer or data processing services to locate their facilities "locally," are not new to cloud computing. However, they are particularly harmful to the goals of realizing the developmental and economic benefits of cloud computing. If localization rules force the development of cloud data centers for various jurisdictions, the economic benefits, including business and economic growth opportunities, will be largely dissipated. In many cases, a market will not be large enough by itself to warrant the construction of a dedicated cloud computing facility. In such cases a localization requirement would have the perverse result of depriving the market of cloud computing services entirely.

The rationale for these polices can vary, but a major motivation is the perception that the economic benefits from data processing—including employment and localized knowledge and expertise—are greatest when the processing is done locally. They are typically aimed at all data processors or all providers of a specific vertical processing service. Sometimes these restrictions are targeted at particular vertical industries, such as financial services or payments companies. Some countries have shown a preference for locally-owned facilities or global companies that work with locally-owned affiliates. Regardless, they more greatly affect cloud computing providers who rely on remote facilities to gain an economic advantage over other ways of providing computing services.

Contrary to the goals, localization rules hamper the greatest opportunities for economic gain within local economies. Cloud computing is valuable to a local economy not only—or even primarily— because of the direct economic benefits it provides, but rather because it increases the efficiency and can decrease the cost of computing services. Local businesses are then able to grow, increase productivity and innovation and employment by competing globally. Dissipating these advantages by imposing inefficient and impractical localization requirements will hurt the businesses and enterprises that depend on enhanced computer services to flourish and provide jobs.

The US Government has been embracing the efficiencies and opportunities for cost savings provided by cloud computing, and they have correctly identified localization requirements as an impediment to this goal. For example, a provision in the recently proposed cybersecurity legislation would bar local jurisdictions from requiring the presence of data processing facilities in its local area. In a section about data centers, the Administration proposal said:

> "The Federal Government has embraced cloud computing, where computer services and applications are run remotely over the Internet. Cloud computing can reduce costs, increase security, and help the government take advantage of the latest private-sector innovations. This new industry should not be crippled by protectionist measures, so the proposal prevents states from requiring companies to build their data centers in that state, except where expressly authorized by federal law."[7]

The EU-US ICT trade agreement also correctly discourages this approach. It urges governments not to impose local infrastructure requirements: "Governments should not require ICT service suppliers to use local infrastructure, or establish a local presence, as a condition of supplying services."[8]

Cross-border data flows

From an economic perspective, the unrestricted flow of information allows for the development of an optimal global supply chain. Companies can provide research and development, design, production, sales and support services all over the world. In doing so, companies would like to source from the best suppliers, regardless of country of origin. This optimized supply chain requires that information be able to flow across borders to the greatest extent possible. Some restrictions on the transfer of data are necessary for public policy reasons, but they should be minimized. To the greatest extent possible, the unrestricted flow of information across borders should be allowed.

Cloud computing is a key part of this optimized global supply chain. Cloud firms locate their network facilities where they make the most sense economically and from a networking perspective. This requires them to move data from one location to another without the restrictions that can be imposed by data flow limitations.

Many countries have, or are considering, limitations on the flow of information into or out of their jurisdictions. These restrictions are often imposed for policy reasons related to privacy, security, consumer protection or protection of public morals. For instance, the European Data Protection Directive applies restrictions to the transfer of information about European citizens to countries that lack an adequate privacy regime. Other restrictions prevent online transactions unless the consumer protection laws of the purchaser apply. Certain illegal or harmful content such as Nazi images or defamatory material may not be transferred into other countries. In the recent past, Egypt, Guatemala, Iran, Turkey, China and Vietnam have blocked content deemed illegal or harmful by the government.

The policy issues raised by these restrictions go well beyond cloud computing, and they are not directed uniquely at cloud computing providers. They would apply to content whether it is downloaded to a computer or stored remotely in a "cloud." They would apply whether a company transfers data to its own data center in another jurisdiction or if it transfers the data to a cloud provider with facilities in other jurisdictions.

Governments need to work together to limit the restrictions in this area. For instance, the EU-US ICT trade agreement contains a principle that is a good first step toward this goal. Under the rubric of "Cross-Border Information Flows" it states that "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."[9]

Recommendations for Policymakers

SIIA recommends that policymakers embrace the following key principles in their efforts to develop policies that encourage the economic benefits of cloud computing and ensure that users are protected:

- Avoid cloud-specific rules and policies, in favor of policies that apply broadly to a wide range of technologies and services, and those that maintain a level playing field for cloud computing and all approaches to remote computing and data storage.
- Promote open standards for software and data interoperability, and avoid policies that would favor one particular business model or technology over another.
- Promote policies that allow to the greatest extent possible, unrestricted transfer of data across borders.
- Encourage rules governing data to travel with the data in order to adequately recognize varying jurisdictional requirements, and ensure data subjects do not lose protection when their data is stored and processed in "the cloud", or in any remote computing environment.
- Avoid localization mandates, or any policies that would give preference to data processors using only local facilities or operating locally.
- Seek interoperable privacy regimes in which countries recognize each other's privacy rules to the greatest extent possible.
- Embrace a global approach to cybersecurity that recognizes the global nature of interconnected systems and provides for data to be protected regardless of where it is located, and that seeks international consensus standards that avoid fragmented, unpredictable national requirements.

VI. Debunking The Myths Of Cloud Computing

Myth One: "With cloud computing, no one knows where the data is located." No. If this were true, it would be impossible to retrieve the data. Data can be stored in one location, moved to another for processing, combined with or linked to data in another, and backed up in still another. The precise location at any given moment in time is less important than the quality of protections and services delivered by the cloud provider.

Myth Two: "Cloud computing is a completely new concept." No. Remote computing has been around since the 1960s. What is new is the scale. The large-scale deployment of broadband has allowed the provision of remote services far beyond what was possible before, and this will allow the industry to naturally evolve toward the provision of more and more services on a remote basis.

Myth Three: "Cloud computing is just the new name for the Internet." No. Cloud services are provided over the Internet, but many other non-cloud services are dependent on the Internet as well. When you download a song from iTunes onto your computer or digital music player, you are using the Internet but not necessarily the cloud. When you store your music in a remote server, such as Amazon's or Google's, and have device-independent access to it, you are using both the Internet and the cloud.

Myth Four: "New legislation is needed to allow the growth of cloud computing." No. Some public policies such as localization laws and restrictions on data flows can hurt the cloud, and they should be avoided. But industry best practices, fostered and encouraged by partnerships with government and civil society and enforced through contract, will address concerns and provide for industry growth.

Myth Five: "Cloud computing is less secure than on-premises data storage." No. Remote data storage has been part of the computing industry for decades and can be made as secure as the customer requirements dictate. Good security practices in centralized data centers can be more effective and less expensive than trying to protect data in every customer's premises.

Myth Six: "The primary employment benefits of cloud computing come from building and maintaining of data centers." No. The primary economic benefit of cloud computing is the boost it can give to other economic activity through the provision of more effective and less expensive computing capabilities. This is especially advantageous for new firms and small and medium sized enterprises, where much of the employment growth can be found. The biggest employment gains for a country or region derive from this more efficient provision of computing services to other businesses and enterprises.

Endnotes

1. Peter Mell, Timothy Grance, "The NIST Definition of Cloud Computing (Draft), Recommendations of the National Institute of Standards and Technology," January 2011.

2. Gartner, Inc., "Forecast: Public Cloud Services, Worldwide and Regions, Industry Sectors, 2009-2014," June 2, 2010.

3. Federico Etro, "The Economic Impact of Cloud Computing on Business Creation, Employment and Output in Europe," May 1, 2009.

4. Ibid.

5. Michael R. Nelson, "Briefing Paper on Cloud Computing and Public Policy, Prepared for the OECD ICCP Technology Foresight Forum," October 14, 2009.

6. To be clear, the notion of open interoperable standards is very different from the idea of free, open content. Open standards will allow, for example, customers to take their data from one cloud provider to an-other. This does not imply that IP owners should allow access to their content for free.

7. FACT SHEET: Cybersecurity Legislative Proposal, May 12, 2011 http://www.whitehouse.gov/the-press-office/2011/05/12/fact-sheet-cybersecurity-legislative-proposal

8. European Union-United States Trade Principles for Information and Communication Technology Services, April 4, 2011.

9. European Union-United States Trade Principles for Information and Communication Technology Services, April 4, 2011.