

## **SIIA Comments: EU Public Consultation on Cloud Computing**

**August, 2011**

### **What kind of barriers do you face in providing your cloud computing services within the EU? Elsewhere?**

One of the greatest current challenges to the application and adoption of cloud computing services are the myriad efforts by governments around the world to develop cloud-specific legislation or regulations. If these efforts continue, there is a real risk that users (either in the enterprise, public or consumer sectors) will be denied the benefits of these services.

Cloud computing covers a variety of technologies and business models, covers both business-to-business service and the businesses that are built on top of cloud services and offered to the general public. Therefore, no single one-size-fits-all policy could apply properly to all these technologies and business models.

Additionally, there are considerable challenges posed by issues surrounding transnational data flows, particularly the challenges associated with conflicts of law and jurisdiction within the EU and beyond. This is not an issue that is specific to cloud computing, but it has been exacerbated by it. Jurisdictional differences in treatment of data have been around for some time, but as provision of computing services become more global in nature, these challenges are amplified. Additionally, the EU Data Protection Directive and Data Retention Directive are unclear in many areas, and they are applied differently among EU Member States. Even in cases where a cloud agreement stipulates choice of law and jurisdiction.

Finally, localization rules, those that require providers of computer or data processing services to locate their facilities “locally,” are not new to cloud computing, but they are particularly harmful to the goals of realizing the developmental and economic benefits of cloud computing. Localization rules would have the effect of dissipating the economic benefits, including business and economic growth opportunities, of cloud computing. In many cases, a market will not be large enough by itself to warrant the construction of a dedicated cloud computing facility, having the perverse result of depriving the market of cloud computing services entirely.

And while not exactly a “barrier” at this time, an open standards-based cloud infrastructure is critical, where opportunities for software and data interoperability are maximized. In this area, the EU should call for open interfaces and standards, wherever and whenever they are available, while avoiding technology mandates of any standards.

**Do you feel that in the cloud services you are currently using or have been evaluating (or are providing), the rights and responsibilities of both user and provider are clear?**

Yes.

**Is there an alternative approach to the determination of jurisdiction that may work better both for users and providers?**

Yes.

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 identify which jurisdictions should prevail and establish 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. Therefore, the rules governing data should travel with the data. 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.

**Do you feel that the question of liability in cross -border situations is clear for cloud users and cloud providers?**

No.

This is one of the areas where the current Data Protection policy in the EU lacks sufficient clarity with respect to transnational data flows. Not only is there a lack of clarity with respect to the process to determine which laws are applicable, but also a lack of clarity with respect to the enforcement by the various Data Protection authorities.

### **Legislative Framework**

**Do you think there are updates to the current EU Data Protection Directive that could further facilitate Cloud Computing while preserving the level of protection?**

Yes.

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 the EU and the US improve on mutual recognition each other's privacy rules to the greatest extent possible.

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.

The EU should support the creation of an effective international data transfer regime that departs from the current geographical location to the recognition of accountability model for transfers of data from the EU to third countries. Such an approach should also prevent EU Member States from requiring additional conditions, such as localization requirements. Such a policy should recognize the country of origin principle as the criteria to determine the applicable law for cloud services customers and the security requirements for cloud service providers within the EU.

Also, cloud service providers and customers are challenged by the potential application of myriad security standards. A more efficient and effective approach would be to reconcile security requirements -- broadly beyond just cloud computing -- and apply it uniformly. The EU should 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.

**Are you aware of specificities in Member State data protection rules, or other legislation, that prevent you from using/providing cloud services within the EU?**

Yes.

For instance, adoption of global cloud computing services are severely obstructed by the application of laws by some Member States to prevent the processing of certain types of data (sensitive data) outside their national territory. Any policies that would prohibit the use of clouds located outside the EU should not be applicable, particularly in cases where the European Commission has issued an adequacy decision in respect of the jurisdiction.

Austria, Greece, Luxembourg, Spain and Portugal require specific approval by the national DPA prior to an international transfer to a Country where there is no adequacy finding by the European Commission, and this approach is extending to other countries. As the EU-US Safe Harbour framework is not (strictly speaking) a Country adequacy finding, this leads to unjustified additional requirements on transfers to or through the US. For example, on June 18 2010, the DPA of the German federal state of Schleswig-Holstein published a press release and a comprehensive legal opinion on cloud computing. The Opinion held that: clouds located outside the EU are per se unlawful, even if the EU Commission has issued an adequacy decision in respect of the jurisdiction. This is additionally problematic because the EU-US Safe Harbor framework has the dignity of an international agreement under EU law (and sanctioned by a European Commission binding Decision), and the provisions within the framework allow for “onward transfer” from the US to other territories, so long as the entity is certified under the framework. Similarly, a DPA in Denmark issued an opinion on February 3, 2011 required “an agreement based on the EU Commission's standard contractual clauses and an application for authorisation from the Danish Data Protection Agency.” There is no requirement under the framework to require contractual clauses or to apply for ex ante authorization from the DPA for transfers that are valid under the framework.

**From your perspective, would it be useful if model Service Level Agreements or End User Agreements existed for cloud services so that certain basic terms and conditions could easily be incorporated into the contractual agreements? If yes, further thoughts about how this might/should work?**

No.

There are a wide range of technologies, platforms and service models that comprise cloud computing. Given this landscape, and the current existence of SLAs and EULAs, SIIA believes that the best approach is for contracts to continue evolving in accordance with market demands.

However, *voluntary* SLAs or End User Agreements could be a way forward and we would encourage the development (or use if developed elsewhere) of a common vocabulary and definitions and potentially standard clauses for voluntary use (so available for use without copyright restrictions on their re-use in legal contracts and legal advice etc), but draw back from providing actual model SLAs and EULAs.

### **Interoperability**

**Please describe interoperability or (data) portability issues you have encountered when using/providing cloud services or are otherwise aware of.**

In many ways, cloud computing is an extension of internet-based computing. Therefore, there are many existing standards that pertain to services within the cloud that ultimately impact cloud interoperability more generally. However, regardless of the specific standards, the movement towards cloud computing has increased the need for open standards for software and data interoperability. 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.

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.

An open standards-based cloud infrastructure is critical, 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.

**Which existing or emerging standards support interoperability across clouds and portability of data (from one cloud to another)?**

At this juncture, SIIA has not yet identified specific standards that are the best for broadly-held objectives to maximize open standards and interoperability. However, SIIA supports

the EU commitment to moving toward true cloud computing interoperability, cloud solutions whose data and corresponding software applications can enable communications and information sharing, seamlessly and in real-time, as appropriate, within and across government and its constituents. The use of non-proprietary data formats and open APIs is critical for cloud computing interoperability. The EU should avoid technology mandates of any standard. Instead, the appropriate role would be to call for open interfaces and standards, wherever and whenever they are available.

There are certain aspects of cloud interfaces, such as storage as a service, which could be invoked across clouds for which standards are emerging. At a minimum, fully and completely disclosed, and effectively implementable APIs are a first essential element for interoperability that providers need to support. Interoperability among the various clouds will be a crucial enabler for the continued growth of innovative applications.

**Which are the most important standards that are currently missing but which you feel are necessary to ensure interoperability and portability? Please describe in detail the aspects they should cover?**

Again, SIIA has not yet identified specific standards that exist or areas where more work needs to be done. However, SIIA believes that Governments have 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.

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.

Today, there are multiple private sector-led efforts to help advance standards for cloud computing to achieve this interoperable vision for cloud computing. Importantly, 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.

### **What can the public sector do as a cloud user to support the emergence of best practices?**

As stated above, the public sector can play a very positive significant role participating in multi-stakeholder processes and sometimes as a convener of such processes. Additionally, the EU should emulate the U.S. Government's effort to encourage, accelerate and facilitate public sector adoption of Cloud Computing. Beginning in 2009 with the launch of its Cloud Computing Initiative, an effort to identifying the potential of cloud computing to greatly reduce waste, increase data center efficiency and utilization rates, and lower operating costs across the Executive Branch, the U.S. Government has made great strides towards adoption of Cloud Computing.

### **Public sector clouds**

### **What can the public sector do as a cloud user to support the emergence of best practices?**

The public sector can play a significant role participating in multi-stakeholder processes and sometimes as a convener of such processes. The EU should emulate the U.S. Government's effort to encourage, accelerate and facilitate public sector adoption of Cloud Computing. Beginning in 2009 with the launch of its Cloud Computing Initiative, the U.S. Government has made great strides towards adoption of Cloud Computing.

With respect to the government procurement processes, this should be vendor and platform neutral to ensure a level playing field when it comes to providing cloud services. Policy efforts should seek to encourage effective cloud computing and maximize the benefits that cloud computing has to offer through full and open procurement processes. Public-procurement processes should be open and transparent, and should require that all bidders provide a clear path for standards-based interoperability, and to provide for data portability so that the public agencies are not locked in to any particular technology or vendor.

### **Please elaborate in particular on public procurement of cloud services.**

Again, this is an area where the EU and other governments can emulate some sound recent policies by the US Gov. Recently, the US Gov. correctly identified localization requirements as an impediment to its goal of advancing cloud computing. In the recently proposed cybersecurity legislation put forth by President Obama, it was explicitly stated as an objective to 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.”

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.”

### **Global solutions for global problems**

#### **What are the most important Cloud Computing problems that have to be discussed at global level?**

As discussed in more detail in our answers to the previous questions, the greatest challenges to cloud computing mostly derive from the application of existing and proposed public policies that could hurt the development of cloud computing—of course, most of these challenges are not new, and not specific to cloud computing. The challenges include restrictions of cross-border data flows, requirements for the location of computer facilities, and application of differing privacy and security policies. Additionally, while there has been much progress in the area of developing open standards, there is still more work to be done in developing an open standards-based cloud infrastructure, where opportunities for software and data interoperability are maximized by open standards.

#### **And which would be the right fora/approaches to tackle them?**

SIIA is supportive of the multi-stakeholder approach adopted by the U.S. Government, led by the NIST, as discussed above. While this effort is largely driven by U.S. entities, there is an opportunity to build-on and expand such initiatives to encourage international collaboration, particularly with the goal of facilitating the transmission of secure cross-border data flows.

Additionally, international organizations such as the Organisation for Economic Co-operation and Development (OECD), represent the right framework for policy making and discussion. Other areas where there is significant ongoing progress include the transatlantic dialogue initiated at platforms such as the ASPEN Institute IDEA (International Digital Economy Accords).