Keio University

1858

CALAMVS GLADIO FORTIOR

Asia Cloud Manifesto

November 2010

Junghoon KIM, Keio University

Tomoaki WATANABE, Center for Global Communications

Naoto IKEGAI, Keio University

Published by:
Keio Research Institute at SFC
Platform Design Laboratory
5322 Endo, Fujisawa 252-0882, Japan

Asia Cloud Manifesto

Executive Summary

Cloud computing holds the promise of enhancing economic, political and cultural interdependence among Asian nations by dramatically accelerating cross-border information and services exchange. Just as coal and steel formed the basis for European cooperation after World War II so too information or “bits” can assist in enhancing overall economic growth and potentially growing regional integration within Asia. Opening a dialogue among the leading universities in and out of the Asian region can help stimulate and shape increased cooperation among and between governments and industry in identifying issues and defining solutions to promote cloud computing within Asia and to assist in the greater integration of these efforts globally.

The advent of the cloud provides multiple challenges and opportunities for Asian countries. The cloud further opens the door for Asian businesses to compete globally and to improve the delivery of health and education services on a national and regional basis that are fundamental to future economic growth and social development. The successful development of cloud computing throughout Asia also depends on the development of a regional market for both services and innovation. An Asia-wide market for cloud services offers the potential for huge economies of scale that can drive increasing higher levels of service delivery. Yet fully realizing this potential will require greater efforts to harmonize laws related to services such as data hosting, data transfer and storage.

Moreover, the challenges are not simply legal and economic. The reality in many Asian countries of state intervention in the provision of cloud services in the name of national security will not change soon. The requirements placed on cloud service providers become particularly complex once multiple jurisdictions are involved and it becomes difficult to determine what set of rules apply. Actions by national governments in Asia competing to attract cloud computing businesses could also prove problematic if there emerges a “race to the bottom” with countries lowering standards such that the rights of consumers are disregarded or foregone.

Co-regulation with government, industry and outside groups, such as the university and NGO communities, playing a role and sharing responsibilities may offer a balanced way forward in regulating the cloud, permitting the flexibility needed for the further development of this rapidly evolving technology. The challenge is clearly how to move beyond national frameworks and begin exploring regional cooperation. Within this context, regional trade associations and international institutions have a role as do multinational firms and NGOs.

Among the issues that need to be addressed as priority concerns are privacy, competition policy, standards-setting, security, data sovereignty, and copyright And while some of these issues are not exclusive to the cloud, beginning cross-jurisdictional discussions now in the context of cloud computing developments can create the necessary environment for confronting and resolving issues as the grow.

Recently awareness as to the importance of cloud computing has been growing rapidly within the academic communities in Asian countries. Creation of an international "Asia Cloud Academic Forum," embracing centers of excellence and researchers across Asia and beyond, can help foster a multidisciplinary academic research stream with an international dimension. The Forum can help broker collaborative efforts designed to explore how Asia might be a driving force globally for innovation in cloud computing, building on the cooperative relationship recently established between Keio University's Global Internet Economy Institute and Harvard University's Berkman Center for Internet and Society.

■1. The Implications of Cloud Computing for Asia

The countries of Asia have rich resources, including both manpower and material assets. Yet they have been unable to leverage these assets to achieve closer regional alignment due to cultural and linguistic barriers, a history of colonialism and differences in political systems rooted in the East-West conflict during the Cold War. But these territorial barriers are becoming more porous as interaction occurs over the cloud and

across boundaries. The development of cloud computing holds the potential to greatly further enhance the economic, political and cultural interdependence among Asian countries – the challenge is how to achieve this.

Cloud computing is not a single, fixed concept. A broadly-used definition by NIST (National Institute of Standard and Technology) in the US states that cloud computing is *a model* providing quick provisioning and release based on limited external management by, and interaction with, service providers and enabling simple, on-demand access to scalable computing resources, e.g. networks, servers, storage, applications, and services[1]. The cloud is also *a framework* for integrating the latest technological and service components on the network and making them available in a simple and quick manner.

Viewed in this context, for Asian countries to benefit and prosper they will need to strive to both provide the components for the cloud *and* to integrate them to deliver services via the cloud. If Asia is to redefine its economy in terms of the cloud, companies and countries in Asia need to reposition themselves not just as users of the cloud but as providers of cloud services and drivers of innovation. The expansion of cloud computing in Asian countries stands to drive and deepen complex changes in economy and society. The underlying technologies for cloud computing and cloud-based services have the potential to open new avenues for growth and new opportunities for regional cooperation over the next ten years.

The first big trend is the ongoing democratization of computing, which cloud computing will further broaden and accelerate. One group that stands to be a prime beneficiary of the development and uptake of cloud computing are SMEs. Asian economies, particularly those in Southeast Asia, are disproportionately comprised of SMEs, and they have driven much of the regional growth over the past 50 years. But while Asian economies are growing rapidly, many countries continue to be held back by the lack of human and infrastructural resources for large-scale computing – a constraint that cloud computing could address. Additionally, in an information-led society,

[1] NIST Definition of Cloud Computing v15 http://csrc.nist.gov/groups/SNS/cloud-computing/

unlike in earlier eras where heavy industry dominated, successful services do not need to be based on large capital spending and expensive research. There are many instances where small- and medium-sized companies and entrepreneurs can win customers through the provision of innovative services based on new business models

In this regard, a key value of cloud computing for Asian economies is the further momentum it can provide to cloud-services businesses in enabling local entrepreneurs to compete globally. The cloud opens opportunities not only for Asian countries already on the path to growth, but also for those still on the road to sustained development. With the rapid proliferation of network-enabled PCs, now widely available for less than $500, and perhaps more significantly, mobile devices, cloud computing stands to broaden and accelerate the access to and delivery of services, and to stimulate entrepreneurial activity.

A second trend is the role of the cloud in the public sector including administrative services, health care and education – and the contribution it can make to enhancing government effectiveness and promoting greater efficiency and transparency. Administrative services in many Asian countries suffer from low productivity when compared with the more dynamic private sector due to bureaucratic rigidity and a lack of professional services education and opportunity. Redesigned workflows and greater transparency achieved through the deployment of cloud-based e-Government services can positively reinforce similar developments in the private sector, creating a virtuous cycle.

In the area of health care, many in Asia are still unable to receive adequate medical services due to the lack of doctors and medical facilities. Developed countries like Japan also need to cope with the increasing burden of health care cost caused by aging populations. Remote health care based on cloud and the advancement of preventive care based on electronic health records (EHR) should enable the delivery of health care and public health with lower costs, higher quality and better medical outcomes. The cloud also portends significant changes for education, enabling distance education in developing countries from university centers in the region. Education is an area that requires more attention and discussion within academic circles if the possibilities

offered by the cloud are to support the creativity and innovation required by information-led economies.

■2. Greater Regional Cooperation on the Cloud

Given the opportunities presented by the development of the cloud, both to overall Asian economic growth and to individual economies, a specific focus on the requirements for creating a regional market in Asia to support cloud computing activities is needed. The realization of a dynamic cloud ecosystem in Asia will afford new economies of scale as well as support for new social values. But there are many barriers to success in this area, both within and between countries. Greater dialogue and debate is needed at the national, regional and global levels if the necessary environment is to develop within Asia and into the broader global economy.

2-1. Economies of Scale

The economic benefits emerging from the creation of a regional market based on the cloud in Asia center to some extent on new multi-tiered economies of scale that can drive innovation and consumer value. An Asia-wide market for cloud services offers the potential for significant economies of scale, both in terms of infrastructure (computing capability and storage) and the diversity and dissemination of services.

Large scale cloud computing creates an environment where multiple servers can be accessed by a single or multiple users at the same time in a secure manner. In the so-called public cloud, there is a usage environment where computing resources are seamlessly shared among many users allowing them to draw on as much or as little as they need. The efficient sharing of, and access to, computing resources that this enables, reduces the initial cost barriers for businesses, promoting new market entry and far greater innovation.

But many cloud solutions offer more than just raw computing, making possible a range of services and various programming environments, including robust security, analytics and account settlement. Cloud computing is thus more than just a utility. It facilitates

service delivery in a wide range of ways, greatly shortening development times for new business and reducing ongoing management and operational costs. And, since it is almost infinitely expandable, as more businesses share a cloud platform, the barriers to entry and the cost go down, not up. Such economies of scale promote market expansion as well as common service standards and interoperability.

The benefits of these economies of scale do not pertain only to service providers. Consumers benefit enormously as well. When service providers can offer cross-border services and attract users in multiple countries, they can further increase their investment in innovation. The larger market allows providers to create niche (i.e., long-tail type) services which would not pay in a smaller market, and to develop services tailored to the individual rather than just mass market requirements.

The increasing number of users made possible by the cloud also contributes to the enhancement of service contents. For example, the “life log” business which is based on various user data such as location data, buying data and behavioral data, enables cloud service firms to provided tailored recommendations on products and services to individuals. Success and accuracy, however, is heavily dependent on the number of users of the service. And in the area of healthcare ICT, initiatives are underway to statistically analyze the accumulated health and behavioral information of consumers and leverage it for the development of new treatments and drugs. The growth of a regional market for the creation, delivery and consumption of “cloud” services in Asia has great significance in that it holds the potential to transform volume transactions into value-added services.

The proactive development of cloud computing in Asia will incubate and draw in a large number of service providers, and the service delivery benefits will in turn nurture a new group of consumers with real purchasing power. Indeed, there is an opportunity for Asia to lead the world based on the cloud, but the region must take the steps necessary to create an environment that will draw in service providers and consumers both locally and from around the world.

2-2. Interoperability

There are also many issues to overcome if Asia is to benefit fully from the potential of cloud computing. Probably, the biggest barriers are the inconsistencies in legal and regulatory systems among nations. There are various laws and regulations in each country for services such as data hosting, data transfer, and data delivery. Yet, it is the nature of cloud technology that data be hosted on multiple data centers and for data to be delivered to customers located outside the countries where data centers are located. It is also a basic requirement that data be delivered through third parties dealing with multiple customers and end users.

The Internet has increased cross-border trade relations and this is only going to accelerate with cloud computing. The delivery of cloud-based services not only involves a relationship between service providers and service users, but also new layers of intermediaries, such as cloud operators who offer computing resources to service providers, and the underlying data centers that will often be located outside the countries where the providers and/or recipients are located. The legal implications created by these conditions are vastly more complex than current bilateral trading relationships provide for.

Thus, despite the advances in technology, arrangements are not yet in place in Asia to provide adequate convenience and transparency for businesses and end users using the cloud. If these issues of jurisdiction and applicable laws are not solved, the potential for cloud computing to facilitate new market entry and to enable various innovations will be seriously undercut in the region. The differences between countries in defining various interests based on property rights and personal rights and in setting the procedures for investigation and policing by state authorities are complex questions.

The issues are also related to interests of national security and measures against transnational terrorism. Especially since the 9/11 attacks, Western nations have introduced laws and regulations to monitor all manner of communications, including cloud-based services. In Asia, these practices are even more prevalent. These legal requirements for state monitoring and censorship are deeply rooted and will not be easily modified, making international coordination difficult. Yet, the ever expanding

levels of confidential information traversing the cloud, both personal and corporate, including email and healthcare information, means that the interests of the State could potentially become a significant obstacle to increasing levels of cross-border information delivery through the cloud.

2-3. Freedom of Expression

It has been one of the major challenges from the start of the Internet as to the appropriate role of service intermediaries, e.g. what responsibilities intermediaries should shoulder for user-initiated fraudulent activities such as copyright infringement, the leaking of confidential information, and defamation. Intermediaries include Internet service providers (ISPs), server operators, and the providers of UGC (User Generated Content) services including bulletin board services (BBS) and video-sharing sites. To this list must now be added cloud operators who are going to be increasingly influential intermediaries both in terms of quality and volume of material delivered across the Internet.

The issue of what responsibilities intermediaries should shoulder will significantly impact the activities of cloud operators, influencing the development of cloud computing and cloud-based services and inevitably shining a spotlight on what constitutes freedom of speech. Having intermediaries shoulder excessive responsibilities, i.e., making them liable for civil and criminal penalties, otherwise applied to the entities that have committed fraudulent activities, can make service delivery tremendously difficult and block the healthy development of an information-led society.

Many legal revisions to at least partially limit the responsibility of intermediaries are currently being considered in the United States, including the revision of the Digital Millennium Act and the introduction of a national Communications Decency Act. A similar process is underway in the EU with the enactment of the Electronic Commerce Directive. In both cases the objective is to strike the right balance between rights holders and the service conditions of intermediaries. The focus appears to revolve around variations of “notice and takedown,” i.e, intermediaries taking a quick action to delete contents based on formal request made by rights holders. Asian nations may

want to consider these arrangements as a model.

The development of cloud computing, however, can bring about issues that cannot always be dealt with by limiting the responsibility of service intermediaries. The expansion of the cloud and the increasing sophistication of the technology make it possible to block the distribution of certain information in advance on request. The targets include not only application providers, such as UGC service operators, but also data center operators hosting services and possibly the operators of specific DNS servers. If even one of these intermediaries accepts a claim of rights infringement or decides unilaterally not to disseminate certain information, the flow of information on the cloud can be disrupted.

The more intermediaries there are in the distribution chain, the greater the possibility that information distribution on the cloud can be restricted – and by implication the basic right of freedom of speech. Since intermediaries operating on the cloud are not necessarily located in the same country, the restriction on expression can be influenced by those countries that are most sensitive to these issues or most willing to take action to restrict the flow of information. And in instances where multiple jurisdictions are involved, it is impossible to determine what set of domestic rules should prevail.

2-4. Competition

The harmonization of laws and regulations related to cloud computing may well occur over time through institutional competition among nations for the location of data centers and cloud-based services dissemination. In this regard, large international companies are at an advantage since they can set server locations and service areas on their own to a certain degree. However, it is small-and-medium companies that are often important initiators of innovation in the area of ICT, and without government recognition of their role – and potential – in cloud development, they risk losing out in this competition.

Differences in legal and institutional environments can have a great impact on the selection of locations for data centers and service operations and the selection of service areas. Risks include the possible seizure of servers by state authorities for failure to

cooperate with information requests as well as possible customer boycotts in other jurisdictions when such cooperation is given. Thus, there is a strong incentive to avoid countries where there is excessive regulation of cloud-related activities. .

On the other hand, a number of governments in Asia are beginning to craft domestic laws to protect cloud service businesses operating within their borders out of a desire to be competitive in the cloud computing market. They are following the examples of locations such as the State of Delaware in the US, which has attracted the headquarters of many American corporations with its highly favorable and predictable legal environment, and the Cayman Islands, which draws financial firms from around the world with its low corporate tax rate. While this kind of competition is desirable, it is also important to avoid a "race to the bottom," whereby some countries create a judicial vacuum and forego consumer protection, thereby sacrificing trust in cloud computing in the long term, in order to maximize their own short term interests. Striking a balance will, of necessity, require significant international coordination. As such, Asia needs to begin looking at the elements required to create an innovation-friendly environment for cloud computing through a balance of coordination and competition.

■3. Regulatory Policy Direction

It is increasingly necessary to develop appropriate legal policies and achieve greater policy coordination and harmonization among Asian countries so that new cloud-based technologies and services can be rapidly deployed. Cloud computing is a general purpose technology that enables a wide range of services, but is also a technology that engenders a wide range of social and economic issues, which require urgent attention, such as privacy and security. Specific issues will be addressed later, but at this juncture it is useful to consider the basic direction and framework for regulation and policies on cloud computing.

3-1. Governmental Regulation, Self-Regulation, and Co-Regulation

Government regulation probably comes first to mind in considering a regulatory framework for cloud computing. However, the development of information

technologies, including the cloud, makes it difficult to establish and enforce specific measures due to the rapidity of technological advance. Moreover, very breadth of the cloud and services operating on it reverses to some extent the usual asymmetry of information between the public and private sectors and underscores limits of national regulations and policies in a global environment.

Under these circumstances, "self-regulation," which relies on the development and enforcement of rules by private organizations, becomes an increasingly functional alternative. Self-regulation is usually led by trade associations representing specific industry segments and has generally been employed to avoid the introduction of new regulations demanded by the public or to provide oversight in an area at the request of the government. Typically, self-regulation has been relied on to restrain direct supervision of sensitive areas related to freedom of expression, such as broadcasting.

The expansion of cross-border information delivery and the sophistication of services being delivered by the cloud are only going to exacerbate many conflicting regulatory issues, raising the question of whether self-regulation based on private-sector initiatives could play a greater role moving forward. However, it needs to be recognized that self-regulation itself can be problematic, e.g,. How can transparency be maintained? Will the existence of free riders undermine the effectiveness of the rules? Does self-regulation under rules defined by existing operators limit market entry for new competitors? What accountability is there in the case of abuse? These issues will become ever more urgent and complicated as cloud computing enters into areas of confidential and sensitive information, such as health records.

As a result, there has been growing interest recently in the concept of co-regulation, which has self-regulation as a basis, but also includes a more explicit role for government. Co-regulation is neither self-regulation nor governmental regulation. Instead it takes the advantages offered by these two approaches to create a collaborative structure between the private sector and government to achieve specific policy goals. How and when the government intervenes under this set of rules differs depending upon the nature of the issue and the structure of the targeted industry.

In Japan, a co-regulatory approach was ultimately adopted in the context of Diet consideration in 2008 of a bill to mandate “filtering” of sites deemed “illegal” or “harmful”. The issue was clear-cut with respect to “illegal” sites, for example, those involved with child pornography or fraud, but the distinction was less clear with respect to the definition of what might be regarded as “harmful.” As such, empowering the government to make and enforce these provisions raised concerns with restrictions on freedom of expression. Ultimately, an acceptable compromise was reached whereby a private association was empowered to create “voluntary guidelines” as a reference for the industry. Programs to educate children and parents about potential dangers on the Internet were also put in place.

Related to this issue of online safety were discussions in Japan regarding the context of the revision of the telecommunications and broadcasting laws to introduce certain public service and content restriction provisions to the regulation of the so-called “content layer”. These proposals drew strong concerns and the government has withdrawn its proposal.

3-2. Global Public-Private Co-Regulation

The challenge is for each country to establish a framework for public-private co-regulation in order to protect safety and security on the cloud while preserving innovation. To date, most of the existing co-regulation initiatives have been limited to domestic activities based on the collaboration between local trade associations and the national government. A goal should be to create and promote a co-regulation framework covering the whole of Asia and ultimately the globe to enhance cross-border information exchange and international collaboration based on the cloud. Currently, there are a variety of issues related to cloud computing being worked on independently by various groups. The challenge is to try to knit these together into a broader more collaborative framework. While the cloud is a relatively new technological construct and we have a lot to learn about how it can be regulated, there are many lessons can be drawn from our experience in regulating and responding to similar issues related to the Internet. Some examples at various levels follow:

(1) Leadership by international organizations

International organizations are just beginning to get involved with cloud-related issues. A concern is that rulemaking in these forums can lack the flexibility and enforceability of domestic legislation and thus may not always be the best vehicle for international collaboration on the cloud. Experience suggests that non-binding guidelines may be a better approach. For example, the recent initiative by APEC on the cross-border protection of personal information is significant in this regard. The APEC Data Privacy Pathfinder Projects,[2] started in 2009, consists of self-assessment guidelines for national cross-border privacy rules (CBPR), a certification guidelines project to establish a structure to certify CBPR-compliant operators, a CBPR compliance review project to define review procedures for certified organizations, and other projects. In addition to these projects, the Organization for Economic Cooperation and Development (OECD) provides a "Privacy Statement Generator" where private sector organizations can easily create their own privacy policy in line with the eight OECD personal information protection principles. This is just one example of an incremental but significant growth of assistance for voluntary initiatives on the part of international corporations and associations.

(2) Leadership by regional trade associations

National trade associations are active in the sphere of co-regulation on the Internet and this role might carry over to the cloud. For example, they have been closely involved for years on the issue of illegal and indecent content on the Internet, since it not always easy for end users to locate and contact intermediaries and get them to delete offensive content. Trade associations for ISPs and others have taken a leadership role in offering hotlines to receive complaints and to pass this information to companies for action. INHOPE[3], implemented as a part of the Safer Internet Program in the EU, constitutes an international network of such hotlines in and outside the EU, with the goal of enhancing the effectiveness of voluntary initiatives taken by groups at the national level. Although the focus here is the Internet, this may also be a model for cooperative efforts on the cloud.

(3) Leadership by individual firms

[2] http://aimp.apec.org/Documents/2009/ECSG/SEM1/09_ecsg_sem1_027.doc
[3] https://www.inhope.org/

There is also a trend among global cloud-services companies operating across different countries with vastly different legal environments, to set their own rules of self-regulation with respect to service content provision. For example, Microsoft defined a set of data gathering principles in 2008 which it uses as an operational guideline for global services deployment. Self-regulation driven by specific companies can also be seen in the area of SNS development. In 2008, the EU enacted the "Safer Social Networking Principle"[4], a set of self-regulation principles for youth and privacy protection, in collaboration with major SNS operators in Europe. The principles laid out general rules that applied to all member companies. The main pillar of the principles is a self-declaration by each service operator that specifies its initiatives related to privacy and youth protection in line with its service content. An approach whereby coordination and monitoring of self-regulation rules is supported by government agencies, yet respects the autonomy of individual businesses may be a useful framework for establishing international co-regulation.

(4) Leadership by NGOs

The stakeholders in co-regulation not only include governments and corporations but also consumers and ordinary citizens. International NGOs and NPOs represent their interests and can take leadership roles in setting rules. In the early days of the Internet, the underlying rules and architectures were created and developed by NGOs, which were neither governments nor corporations, e.g. the Internet Engineering Task Force (IETF) and the Internet Corporation for Assigned Names and Numbers (ICANN). NGO participation in co-regulation is not limited to just defining rules. They can also monitor the effectiveness of corporate self-regulation, and offer suggestions from the perspectives of citizens and consumers. NGO participation is vital in all aspects of self-regulation from definition to execution to monitoring. NGOs are also well placed to facilitate discussions between trade associations and governments in order for global co-regulation to become accepted broadly in international society.

[4] Safer social networking: the choice of self-regulation
http://ec.europa.eu/information_society/activities/social_networking/eu_action/selfreg/index_en.htm

■4. A Cloud Agenda for Asia

There are a number of issues that are essential to the future of cloud computing which should be addressed as a matter of priority within the Asian context. Effective solutions will require reconciling 1) maximizing innovation through cloud-based global co-regulation, and 2) the promotion of security, safety, and trust towards the cloud, especially for individual consumers.

4-1. Privacy

It is critical to ensure the trust, security, and safety of both individuals and industry as reliance on cloud computing expands and becomes part of the social infrastructure. A key issue is how personal information protection can contribute to the protection of user privacy, and how this can be ensured in a cross-jurisdictional environment.

There is already a potential international standard based on the eight OECD personal information protection principles adopted in 1980. In Asia, however, a number of countries have insufficient personal information protection laws and regulations. And since the EU Data Protection Directive prohibits data exchange with third countries which do not have in place adequate personal information protection laws and regulations, there is an urgent need to address this issue on a trans-national basis throughout Asia (and indeed globally). Strengthened national laws and regulation *and* a framework for cross-border information exchange through the cloud should be the focus of discussion within the region.

On the other hand, excessive protection of personal information can hinder the free movement of information. There are many gray areas emerging, especially in the ongoing advances in life log-based technologies. For example, some usage scenarios and combining of information capture can infringe user privacy even though they may not meet a strict definition of identifiable personal information. Issues in this context include how the handling of cookies are used as identifiers for fragmented personal information, terminal IDs assigned to computers and mobile devices, and the protection of subscriber IDs obtained at the time of registration for various services. Yet, while regulation may be necessary, these personalized cloud services and the technology they

rely on are still in state of flux. And, as such, premature regulation should probably be avoided. While a rigorous protection standard is required for sensitive information, such as medical records, in many cases self-regulation may assure sufficient anonymity and security. The key is to take a flexible approach depending on the type of information involved.

4-2. Competition and Standards

Cloud-based services and, in particular, the infrastructure and platform layers on which they rest, require strong economies of scale and network externalities if they are to provide a viable return on investment and develop successfully. However, supporting this development may lead to a monopolistic market situation. Of special concern are cases where user data held by one cloud-based operator is locked-in due to an exclusive service business model and cannot be easily ported over to other services -- thus blocking of market entrants or impairing the convenience of users. Thus, while excessive government intervention should be avoided, regulatory authorities also need to consider the applicability of anti-monopoly statutes and the necessity to mandate data portability while closely monitoring competitive status.

Since the cloud environment embraces many technological components and protocols, including for data storage formats, there is increasing interest in standardization and many countries are creating consortiums for precisely this purpose. The role of government through its procurements is clearly important in promoting an open standard-based cloud environment. As governments enhance their role as users of the cloud, the cloud technologies adopted by governments will have a competitive edge as technological standards.

However, rapid standardization and excessive integration can also decrease competition by prematurely freezing standards development, thereby limiting technology advance and innovation. What is needed is an international framework comprised of national governments and international organizations that can support entry by new service operators while proceeding with competitive standardization based on de facto technologies.

4-3. Network Neutrality

The nature of cloud-based services requires continuously connected Internet access. Especially for services requiring stable and high-capacity bandwidth, such as remote healthcare and high-quality video services, equal access to infrastructure has great importance. This is the issue of network neutrality, i.e. whether owners of communication infrastructure should be allowed to discriminate among service providers. And, in the cloud environment, this is a serious concern for cloud service operators. Moreover, there is the related question of whether dominant network providers that also provide "social" infrastructure might favor their own services in a nontransparent manner.

The issue of neutrality cannot be solved by taking sides. The free management of services is an important right granted to each operator and the profitability that comes from strategic alliances with certain operators can help support further investments in infrastructure and contribute to the development of both the communications and cloud environments. The key to making this work is to set up policies that set conditions for preferential treatment and that ensure choice for users through a mix of competitive policies.

4-4. Security

Given the increasing level and array of personal, confidential or otherwise sensitive data that will be stored and transacted in the cloud, data and infrastructure security is one of the major considerations in the development and deployment of cloud services. There is a need to establish broad and sophisticated security standards covering privacy, retention of confidential information, and stable service delivery, if we are to promote information delivery in Asia and gain trust from outside the area as the epicenter of cloud computing. There are many security standards including ISO and ISMS (Information Security Management System), but there is not yet a comprehensive security policy since cloud technologies and services are still being developed.

Asian countries need to implement further initiatives to nurture establish regional international standards. Since ensuring desirable security standards depends on how services are delivered, there is a corresponding need to establish an effective

governance structure based on public-private collaboration, including periodic audits conducted through independent third-party organizations. In particular, it is important that cloud service providers have their compliance with security standards and policies verified through independent, third party audits.

The issue of security is not limited solely to computers and networks. Security heavily depends on social infrastructure aspects, including user awareness, compliance issues, the reliability of power supply, and the telecommunications environment. Solutions should be implemented from the perspective of broad cloud promotion policies encompassing regulation, human resources development, and infrastructure construction, maintenance and protection.

4-5 Sovereignty

The growth of online services has seen a corresponding increase in the level of online crime and threats to public safety or national security. With the growth of cloud computing, there will be an increasing pressure on governments to access the data held by cloud service providers. While multiple jurisdictions may have an interest in a single matter, each seeking access to user information; there are no universally agreed upon rules governing such access by law enforcement. The result is that service providers are increasingly subject to divergent, and at times conflicting, rules governing jurisdiction over user content and data. Further complicating the problem is the fact that different jurisdictions often have different laws regarding privacy rights and data retention.

This thicket of competing and conflicting laws in Asia presents a significant obstacle to the delivery of cloud services that meet users' reasonable expectations of privacy. In cases where the rules of different nations conflict, a cloud provider's decision to comply with a lawful demand for user data in one jurisdiction may place a provider at risk of violating the privacy or other laws of another jurisdiction. Equally troubling, this situation makes it extremely difficult for providers to give their customers accurate and adequate notice of the conditions under which their data might be accessed by law enforcement.

International legal instruments for the sharing of information have so far proven slow and cumbersome, and they have encouraged some countries to begin to ignore established procedures and simply demand that local employees disclose data regardless of where it is located or to which jurisdiction the relevant service is provided.

Today in Asia, there is an opportunity to provide greater clarity and consistency on the legal norms that will protect the privacy and security of user data while also ensuring legitimate law enforcement needs are addressed. To achieve this objective, governments can take several steps such as including these issues into existing dialogue on trade negotiations or pushing for enhanced mutual legal assistance treaties, which could, in turn, help harmonize domestic legislation regarding data privacy issues. Progress made on the ASEAN-Australia Development Cooperation Program on harmonizing e-commerce legal frameworks and the APEC Privacy Framework and Pathfinder Projects provides a solid platform for further development and addressing of the divergent jurisdictional approaches to technology policy.

Whatever option governments in Asia and elsewhere take, it is absolutely essential that these deliberations include not only representatives from law enforcement and justice, but also industry, consumer groups, and other interested stakeholders. Cloud computing will only reach its full potential if providers can establish datacenters and offer services in multiple jurisdictions, without fear that each step will invite competing claims of jurisdiction and government access to data.

4-6. Copyright

Currently, copyright protection is carried out largely through “notice-and-takedown” requests to intermediary services, such as ISPs. But, especially in relation to copyright infringement issues involving UGC services, there is a question as to what extent intermediaries can be required to deploy so-called filtering features, i.e. technologies that “proactively” block illegal and other information deemed “unacceptable” on their services.

Filtering technologies can ensure rights protection at a low cost in so far as they function properly. Yet, with current blocking technologies still far from mature,

information that should not be blocked can be disrupted, and there is a need for a transparent and quick redress process for users whose access is inappropriately blocked. In addition, many laws that define limits to service provider responsibility also explicitly prevent intermediaries from the general monitoring of content. Moreover, this still leaves unanswered the related question of whether "filtering" or "blocking" requirements on the cloud should be limited to just the application layer or extended to the infrastructure (server) or platform layer.

In this context, it is worth taking a note of an instance of "self-regulation" based on a private agreement recently signed between a large UGC service operator and a copyright owner (i.e. a content provider). In 2008, a large UGC operator specialized in video sharing services and a large US movie production company reached an agreement based on UGC principles[5] stipulating the measures to be taken in the case of copyright infringement on the services. This is a "gentleman's agreement" with no government enforcement mechanisms and it stipulates that the content provider will not initiate a lawsuit based on copyright infringement against the service operator, provided that the UGC service provider deploys certain blocking technologies currently available. Of interest is that the agreement also defines the process for responding to users who claim that their content is inappropriately blocked.

Another example, from Japan, has ISPs and copyright owner organizations coming together to create a consortium that sends alert emails to users who repeatedly violate copyright rules in their P2P file sharing.[6] By contrast, the EU recently discussed introducing the so-called three-strike clause to forcibly block an Internet connection for a certain period for users who repeat copyright infringement. However, excessively rigorous measures not only lead to protests from users, but also raise the issue of Internet access as a basic human right in an information-led society. This demonstrates the need for a flexible approach based on agreements among cloud operators, content providers, and users as the most workable solution.

[5] http://www.ugcprinciples.com/
[6] Consortium against Copyright Infringement via File-Sharing Software http://www.ccif-j.jp/

■5. An Asia Cloud Academic Forum

Recently awareness as to the importance of cloud computing has been growing rapidly within the academic community in Asian countries. Creating an Asia Cloud Academic Forum could foster a multidisciplinary academic research stream and link centers of excellence and researchers across Asia and beyond. The Forum would serve to broker and support dialogue within the Asia academic community and promote the establishment of collaborative efforts designed to explore how Asia can be a driving force for innovation in cloud computing.

There is much to discuss and many issues to solve in this Forum, with the purpose of better coordinating cloud-related economic, regulatory and institutional dimensions. As noted already, a clear focus should be on the many legal and other institutional differences between nations in Asia and the obstacles they pose to creating a collaborative framework for the delivery and consumption of cloud services in the region. Regional coordination on legal and other institutional roadblocks can only be achieved through shared perceptions and continual efforts at cooperation based on dialogue between nations. The Asia Cloud Academic Forum can be a place to share both the opportunities and challenges created by cloud computing and propose a common vision for appropriate governance.

One aspect that is of critical importance for Asia going forward is the development of cloud-related human resources. Cloud computing can provide unprecedented opportunities for various companies and individuals to be the initiators of innovation, but the realization of those possibilities requires the availability of high-quality education directed at the effective utilization of information technologies. Entrepreneurs in Asia need more than just technical knowledge. A background in the humanities and social science, an understanding of business management, technology and culture is important as well. A related purpose for the Forum is to help focus government and industry on the need for investment in raising educational standards at university and research institutions and the promotion of research and development. Such a focus on education can also foster a close collaborative relationship between Asian countries, through exchanges between educational and research institutions,

technological collaboration, and financial assistance.

Ultimately, the objectives of the Forum must go beyond the establishment of collaborative relations within Asia. If cooperation on the cloud is limited to Asia, it will ultimately hurt Asian interests and be detrimental to the healthy development of cloud computing globally, since it carries the danger of closed standards and exclusive relationships. It is vital for Asia to make this Forum an open forum for dialogues among universities in and outside Asia. The objective is for the Forum to develop as a vehicle for Asian academic and research cooperation with the world, building on the recent collaborative relationship established between Keio University's Internet and Society Laboratory and Harvard University's Berkman Center for Internet and Society.