Cloud Computing Service and Legal Issues

Takato Natsui

Professor of Law, Meiji University, Tokyo, Japan

1. Introduction

Many IT businesses have indicated that cloud computing is a very promising emerging computer technology and will likely achieve a superior position in network computer technologies . However, there is no widely agreed upon and concrete definition on what constitutes cloud computing. Some may say that cloud computing means SaaS (Software as a Service), and others may define cloud computing as grid computing. In fact, there have been some grid computing based SaaS services via the Internet which have been categorized as 'cloud computing'. On the other hand, some people use 'cloud computing' as a synonym of simple hosting services, data center services or ASP (Application Service Provider) services. Recently, the National Institute of Standards and Technology (NIST) released its 15th redefinition of "cloud computing service"[1] as:

> **Essential Characteristics:**
>
> *On-demand self-service*. A consumer can unilaterally provision computing capabilities, such as server time and network storage, as needed automatically without requiring human interaction with each service's provider.
>
> *Broad network access*. Capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms (e.g., mobile phones, laptops, and PDAs).
>
> *Resource pooling*. The provider's computing resources are pooled to serve multiple consumers using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand. There is a sense of location independence in that the customer generally has no control or knowledge over the exact location of the provided resources but may be able to specify location at a higher level of abstraction (e.g., country, state, or datacenter). Examples of resources include storage, processing, memory, network bandwidth, and virtual machines.
>
> *Rapid elasticity*. Capabilities can be rapidly and elastically provisioned, in some cases automatically, to quickly scale out and rapidly released to quickly scale in. To the consumer, the capabilities available for provisioning often appear to be unlimited and can be purchased

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

in any quantity at any time.

Measured Service. Cloud systems automatically control and optimize resource use by leveraging a metering capability at some level of abstraction appropriate to the type of service (e.g., storage, processing, bandwidth, and active user accounts). Resource usage can be monitored, controlled, and reported providing transparency for both the provider and consumer of the utilized service.

Service Models:

Cloud Software as a Service (SaaS). The capability provided to the consumer is to use the provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through a thin client interface such as a web browser (e.g., web-based email). The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings.

Cloud Platform as a Service (PaaS). The capability provided to the consumer is to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages and tools supported by the provider. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly application hosting environment configurations.

Cloud Infrastructure as a Service (IaaS). The capability provided to the consumer is to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, deployed applications, and possibly limited control of select networking components (e.g., host firewalls).

Deployment Models:

Private cloud. The cloud infrastructure is operated solely for an organization. It may be managed by the organization or a third party and may exist on premise or off premise.

Community cloud. The cloud infrastructure is shared by several organizations and supports a specific community that has shared concerns (e.g., mission, security requirements, policy, and compliance considerations). It may be managed by the organizations or a third party and may exist on premise or off premise.

Public cloud. The cloud infrastructure is made available to the general public or a large industry group and is owned by an organization selling cloud services.

> *Hybrid cloud*. The cloud infrastructure is a composition of two or more clouds (private, community, or public) that remain unique entities but are bound together by standardized or proprietary technology that enables data and application portability (e.g., cloud bursting for load-balancing between clouds).

This may be the most reliable official definition of cloud computing. However, the definition has been revised 15 times, and will likely be, as of the date of this article, revised again in the near future. As technologies used in cloud computing have not been completed yet, more mechanisms, functions and application software will likely be added to current cloud computer models, and fundamental design and usage of cloud computing may be changed and enhanced.

Another definition of cloud computing can be found in a patent application (United States Patent Application 20030051021)[2]. Claim 1 of the patent is:

> **Claim 1.**
>
> A virtualized logical server cloud, comprising: a plurality of logical servers, each having persistent attributes that establish its identity; a network system; a plurality of physical servers, each coupled to physical resources including a network resource for interfacing the network system, a data storage resource and a processor resource, and each physical server executing virtualization software that virtualizes one or more of the physical resources for logical servers that are linked to that physical server; and a server cloud manager, interfaced to the plurality of physical servers, that establishes and maintains status and instance information for the plurality of logical servers including the persistent and non-persistent attributes that link each logical server with a physical server.

As we cannot fix a logically complete and static definition on the term cloud computing, I would like to examine this concept by limiting and observing already implemented cloud computing services in the IT industry.

There have been two different types of cloud computing service offered by the IT industry: one is the public cloud computing service (*cf* the NIST definition) and the other is a private cloud computing service (*cf* the NIST definition). Users of a public cloud can share same resources on the same computer system as their own virtual computer systems. And businesses can hold and manage their private cloud in which employees of the business can share the private cloud system and use their own virtual computer on the private cloud computer system via their local area network system or the Internet. These may look like a modernized resource sharing system of IBM's old VM (Virtual Machine) system. In fact, IBM provides both types of cloud computing service. In addition to such former mainframe computer companies, Microsoft (in the form of Azure), Amazon (in the form of EC2 (Elastic Computing Cloud)) and Google also provide interesting cloud computing services.

[2] See also WIPO Patent Application WO/2003/021396.

These cloud computing services are very useful[3]. However, I believe that the public cloud computing service model may cause some critical legal and computer security issues[4]. These issues arise as a result of the cloud computer being a virtual computer system; users share the same computer resources of the cloud computer, but the authority of the user to manage the cloud computer is inferior to authority of management body (or owner) of the cloud computer service (or system) and the users have control of only a virtual computer and share services but do not control a physical machine or installed application software on that machine[5]. This means that any user of a public cloud computer may be able to control their confidential data on the virtual computer but not be able to control physical system, and similarly can perform an electric audit only on the virtual database system but not on the physical computer system. In addition, every user shares the same resources on the public cloud computer system, but other users of the same public cloud computer may be competitor companies.

In this article, I examine some legal issues which may take place on a typical public cloud computer service mainly in the context of Japanese laws.

2. Personal Data and Privacy Protection

Many businesses have enjoyed the benefits of having data processing and data storage performed on outside computer systems with outsourcing services. Utilizing outsourcing services is a common practice in modern business. As a part of these outsourcing services, personal data is often processed on third party's computer system and stored on yet another outsourced datacenter system.

To ensure reasonable protection of personal information including personal information which is handled in commercial data outsourcing, the Personal Information Protection Act[6] (the "PIPA") was enacted in Japan. Article 22 of the PIPA provides:

> **Article 22 (Supervision of Trustees)**
>
> When a business operator handling personal information entrusts an individual or a business operator with the handling of personal data in whole or in part, it shall exercise necessary and appropriate supervision over the trustee to ensure the security control of the entrusted personal data.

The Japanese central government has announced continuously that the Japanese PIPA is fully compatible with EU Data Protection Directive, however I think it provides less protection for

[3] George Reese, Cloud Application Architectures, O'Reilly (2009)
[4] Gartner: Seven cloud-computing security risks
InfoWorld: July 02, 2008
http://www.infoworld.com/d/security-central/gartner-seven-cloud-computing-security-risks-853
[5] John W. Rittinghouse & James F. Ransome, Cloud Computing – Implementation, Management and Security, CRC Press (2009)
[6] Act on the Protection of Personal Information (Act No. 57 of 2003)
http://www.cas.go.jp/jp/seisaku/hourei/data/APPI.pdf

personal information than does the EU Directive[7]. For instance, Article 17 of the EU Directive provides:

> **Article 17. Security of processing**
>
> 1. Member States shall provide that the controller must implement appropriate technical and organizational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.
>
> Having regard to the state of the art and the cost of their implementation, such measures shall ensure a level of security appropriate to the risks represented by the processing and the nature of the data to be protected.
>
> 2. The Member States shall provide that the controller must, where processing is carried out on his behalf, choose a processor providing sufficient guarantees in respect of the technical security measures and organizational measures governing the processing to be carried out, and must ensure compliance with those measures.
>
> 3. The carrying out of processing by way of a processor must be governed by a contract or legal act binding the processor to the controller and stipulating in particular that:
>
> - the processor shall act only on instructions from the controller,
>
> - the obligations set out in paragraph 1, as defined by the law of the Member State in which the processor is established, shall also be incumbent on the processor.
>
> 4. For the purposes of keeping proof, the parts of the contract or the legal act relating to data protection and the requirements relating to the measures referred to in paragraph 1 shall be in writing or in another equivalent form.

The problematic language in the PIPA is '*appropriate supervision* over the trustee to ensure the security control of the entrusted personal data'. Appropriate control of personal data as computer processed data can be performed subject to well established information security measures, especially utilizing technological ways to maintain confidentiality of the data. This should be exactly same in the context of data processing and data storage on a cloud computer.

For instance, a user ("U") can supervise specific data over virtual system or virtual database, but never control real public cloud computer system ("X") or physical database system. In this case, only owner or management body of X ("MB") has the control on the X and U is one of the users of X. In addition, application software has to be provided from X. Also, even if such software cannot

[7] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data
http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:EN:HTML

adequately protect personal data, U would not be able to remove or repair the application software to maintain adequate protection of personal data, because such application software is shared by every user of X and maintained only by the management body of X under a standard information security management policy. In the world of public cloud computing service, only X's privacy policy and security policy can apply. U's privacy policy and security policy would be inferior in application to X's policies always. In other word, U has no authority to control X or other ability to implement its security protocols should X not comply with U's instructions.

Moreover, in the particular case of grid computing-based cloud computing, user U can know a logical address of virtual database system, but not identify any physical address on an identifiable specific physical hard drive on a physically locating database system. This may be due to a characteristic of grid computing architecture. Also, U and its audit firm cannot sufficiently perform a computer data audit: though they can examine a logical address and logically locate data on U's virtual system and virtual database on the grid-based cloud computer. In some cases, the owner of management body of X may not be able to identify the physical address of U's specific data too. In such a case, U would never have adequate control on any personal information which U is obligated to have control over.

Due to these reasons, a user of a specific public cloud computer service is unable to have adequate control over the physical public cloud computer system and public cloud database system as required by Article 22 of the PIPA.

Therefore, in general, personal data processing and data storage in virtual computer or virtual database on public cloud may be regarded no complying with the personal information protection management obligations set out in the Japanese PIPA.

3. Trade Secret

Trade secrets can be protected under the Unfair Competition Prevention Act[8] (the "UCPA") in Japan. Article 2 (6) of the UCPA defines:

> **Article 2.**
>
> (6) The term "trade secret" as used in this UCPA means technical or business information useful for commercial activities such as manufacturing or marketing methods that is kept secret and that is not publicly known.

This definition provision is similar to that of Uniform Trade Secrets Act (UTSA). Section 1 (4) of the UTSA defines:

> **Section 1. Definitions**

[8] Unfair Competition Prevention Act (Act No. 47 of May 19, 1993)
http://www.tomeika.jur.kyushu-u.ac.jp/ip/legislation/unfair_competition_preventnion_act.pdf

(4) "Trade secret" means information, including a formula, pattern, compilation, program, device, method, technique, or process, that:

(i) derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable by proper means by, other persons who can obtain economic value from its disclosure or use, and

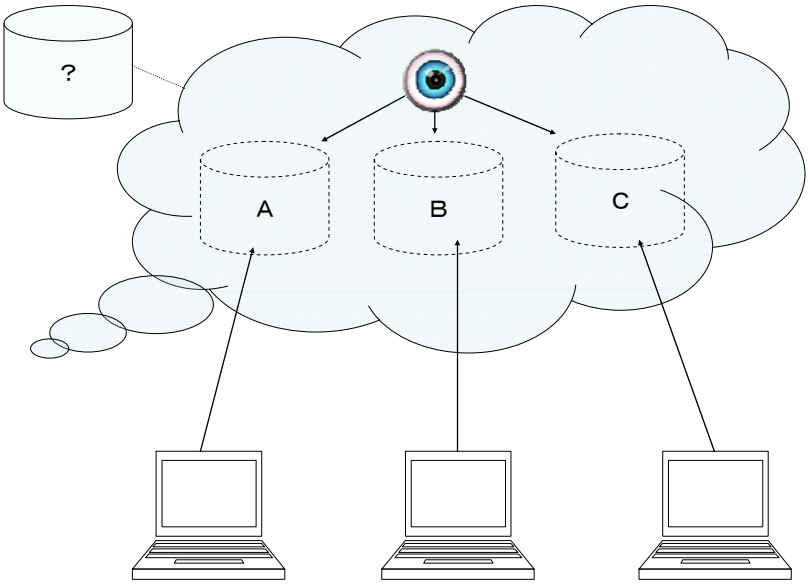
(ii) is the subject of efforts that are reasonable under the circumstances to maintain its secrecy.

The problem with the language in the UCPA is the limitation of definition of trade secret to that technical or business information 'that is kept secret'. In the context of computer data as trade secret information, a 'trade secret owner should also obligate anyone with access to the information to protect its secrecy'[9].

Of course, the information of a user of a virtual cloud computer system can be kept secret, but maintaining such secrecy (confidentiality) is also virtual.
Due to computer security reasons or maintenance of physical equipment of a specific public cloud computer, the management body of the public cloud can examine, confirm, repair or exchange physical hard disks on which user's data may be stored. A user would not be able to block such examination, mending and so on by the management body of the public cloud computer[10].

For example, if a specific user's data was infected by computer a virus or malware was installed on user's (virtual) hard drive then the management body of the public cloud computer would have to remove such security risks; on the other hand such user would not be able to perform such security response because such user is not the root of the public cloud computer. In such a case, the secrecy (confidentiality) of user's information may be compromised.

[9] David W. Quinto & Stuart H. Singer, Trade Secrets, Oxford University Press (2008), p.17
[10] See, Cloud Security Alliance Issues Version Two of Guidance Identifying Key Practices for Secure Adoption of Cloud Computing
San Francisco, CA, Dec 17, 2009
http://www.cloudsecurityalliance.org/pr20091217.html



This is the same even if a specific user's important data has been encrypted, because data encryption application software, when used, is provided by the shared public cloud computing service provider as a part of the shared public cloud computing service, and the management body of the public cloud computing service may have access to the decryption-key for the encrypted data. On the contrary, a user cannot install any different encryption application software into the user's virtual computer on the public cloud computer. Any application software is provided as common shared application software of the public cloud computing service.

For these reasons, it may not be possible to maintain the secrecy of important information on a user's virtual computer on a public cloud computer system even when the user undertakes reasonable effort to maintain secrecy. Therefore, in general, a public cloud computing environment may not be fit for trade secret protection.

4. Jurisdictional issues

The jurisdictional matter is the most problematic issue, not only in the case of cloud computing but also almost every network computer service, because all of the top service providers (especially cloud computing service providers) are American corporations: for instance Microsoft, IBM, Google, Amazon, Cisco, HP and so on.

If a user is located in the United States too then there may be not so many jurisdictional issues, except for interstate issues. However, the legal status of a non-American user is completely

different from an American user. Most service provider service contracts include choice of forum and choice of law provisions. Such provisions can provide the American service provider with a clear advantage over non-American user, by for instance indicating that the courts located in New York City, New York State, the United States shall have exclusive jurisdiction', or that all disputes and controversies arising under the contract 'shall resolved pursuant to the law of the state of Illinois, with United States Federal law applicable as applied in the Northern District of Illinois' and so on.

On the other hand, even if a non-American user of a cloud computing service has a better privacy policy and computer security policy, the user's policies will take an inferior status to the policies of American service provider.

This issue may be one of the most common issues that arises and such common issue should be interpreted and resolved by common legal theories and practices[11]. However, one has to recognize and be reminded that every major cloud computing service provider is located in the United States.

5. Incidents

These concerns have already described by some people[12] including RSA[13] and ENISA[14]. For instance, ENISA noted[15]:

> **DATA PROTECTION**: cloud computing poses several data protection risks for cloud customers and providers. In some cases, it may be difficult for the cloud customer (in its role as data controller) to effectively check the data handling practices of the cloud provider and thus to be sure that the data is handled in a lawful way. This problem is exacerbated in cases of multiple transfers of data, e.g., between federated clouds. On the other hand, some cloud providers do provide information on their data handling practices. Some also offer

[11] See, Jurisdictional Aspects of Cloud Computing
Cristos Velasco San Martin
February 28, 2009
http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/2079%20if09%20pres%20cristos%20cloud.pdf

[12] Guest View: Insurance for the cloud
SD Times: Jan 1, 2009
http://www.sdtimes.com/GUEST_VIEW_INSURANCE_FOR_THE_CLOUD/By_SCOTT_GODES_AND_IDAN_IVRI/About_CLOUDCOMPUTING/34021

[13] RSA's Coviello: Cloud Computing Not Secure Enough
PC World: July 03, 2009
http://www.pcworld.com/businesscenter/article/167841/rsas_coviello_cloud_computing_not_secure_enough.html

[14] Cloud Computing Risk Assessment
ENISA: Nov 20, 2009
http://www.enisa.europa.eu/act/rm/files/deliverables/cloud-computing-risk-assessment

[15] Cloud Computing Risk Assessment, p.10

certification summaries on their data processing and data security activities and the data controls they have in place, e.g., SAS70 certification.

Incident relating to cloud computing services have been anticipated and described in theoretical papers, however in 2009 there were actual security breaches and accidents. For instance, all of the customer data on Microsoft's cloud computing service vanished[16]; Amazon's cloud computer[17] and Google's cloud computer[18] systems were subject to attack by unauthorized installations of malware (computer worm or computer virus).

These incidents may have given us evidence that shows the incompleteness of cloud computing architectures. Cloud computer systems as a physical existence may not be well-established yet, but these systems are essentially a kind of large enhanced ordinary computer system having vulnerabilities similar to ordinary traditional server system. At least, engineers in the cloud computing service providers are the same or similar people as common traditional server system's engineers.

Also these might suggest some difficulties relating to cloud computering. That is, a user has no way to protect and recover its own data stored on virtual database system when the stored data has been accidentally removed, erased, vanished or modified. Only cloud computing service provider has any control authority to protect every data on the cloud computer system.

Compared with traditional individual server systems, this is obviously different. An owner of a traditional server system can entirely control the server system which may involve database systems, and the owner can protect its important information and recover the system and data under its own security management control. However, a cloud computer system is not same as traditional server system. The cloud computer system is similar to an old mainframe computer system which consists of a single main processing system and many DAM terminal equipments such as IBM's VM system or similar machines. Every user of a cloud computing service may look like an operator of DAM terminal machine who cannot install and maintain any computer programs and software, but only use and enjoy already prepared application software on the system.

We have to look at this difference between an emerging cloud computer system and traditional server systems. Also we have to recognize clearly that such a difference may cause an important change of legal framework of network computing.

---

[16] What Microsoft needs to do about the Sidekick fiasco
ZDNet UK: 13 October 2009
http://community.zdnet.co.uk/blog/0,1000000567,10014179o-2000331777b,00.htm

[17] Zeus botnet moves to Amazon for some grid action
The Tech Herald: Dec 10 2009
http://www.thetechherald.com/article.php/200950/4928/Zeus-botnet-moves-to-Amazon-for-some-grid-action

[18] Bot herders hide master control channel in Google cloud-Google AppEngine co-opted
The Register: 9th November 2009
http://www.theregister.co.uk/2009/11/09/bot_herders_coopt_google_appengine/

Similarly, traditional philosophy of management system model and its PDCA method (ISMS[19] etc.) has not yet been able to function, because a user of a cloud computer service is the only one of many customers of the service, but not a management body of the company's computer operation at all. Only the cloud computing service provider has control authority over its whole cloud computer system, and the user only has authority to access to the cloud computer system as an end user.

In addition, privacy certification organizations and information security certification organizations may have lost a lot of certified customers when the customers stopped using traditional independent server systems and changed to only an end-user of specific cloud computing service providers. End-users do not have any control over the physical cloud computer system. Therefore, certification organizations cannot examine any management plans and operations to protect physical computer assets in accordance with the architecture of the specific cloud computer systems, and certify them.

6. Conclusion

Pure grid-based public cloud computer system may provide a contradiction to traditional protection measures including privacy protection laws, trade secret laws and information security management system models.

This is due to a change of fundamental management structure of network computer processing and data storage. ISMS (ISO/IEC 17799-2005) notes:

> The term of 'owner' identifies an individual or entity that has approved management responsibility for controlling the production, development, maintenance, use and security of assets. The term 'owner' does not mean that the person actually has any property right to the asset.

However, although a user may have an intellectual property right in computer data , if the user is a user of a cloud computing service then the user is not 'owner' of its virtual computer on the cloud computer system, because such a user is not an entity who has approved management responsibility for controlling the production, development, maintenance, use and security of assets on the physical cloud computer system at all. The user's control is really virtual and cloudy.

Therefore, if anyone wants to maintain confidentiality of specific computer data for confirming compliance with legal obligating adequate protection laws and protection policies, then using of any pure type public cloud computing service may have to be avoided. Everyone has to choose a better model of cloud computing service where every user can use not only prepared application service on the cloud computer system through a DAM terminal like slave communication machines,

[19] Information technology -- Security techniques -- Code of practice for information security management (ISO/IEC 17799:2005)
http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=39612

but also use the user's own operating system, application software, encryption tools, communication protocols, data storage and other computer resources on their private and independent computer systems and related equipments.

Everyone has to hold independence as a management body and make judgments on important information protection based on their own privacy policy and information security policy in accordance with the relevant laws and legal procedures.