Creating the Environment for the Prosperity of Cloud Computing Technology

Fa-Chang Cheng, Wen-Hsing Lai

Graduate Institute of Science and Technology Law, National Kaohsiung First University of Science and Technology, Taiwan

*Dept. of Computer and Communication Engineering, National Kaohsiung First University of Science and Technology, Taiwan

No. 2, Jhuoyue Rd., Nanzih District, Kaohsiung City 811, Taiwan, 886-7-6011000 ext. 2054/886-7-6011012
e-mail: fachang1@hotmail.com, lwh@nkfust.edu.tw*

Abstract

The key point for the success of clouding computing technology in terms of application is whether such operation can produce the sense of trustworthiness to its users. Technical measurement has always been the fundamental preventive precaution, no matter what kind of aspect in dealing with producing the sense of trustworthiness. Except technical measurement, there are two developing issues surrounding the central idea worth notice, which is the protection of information privacy and the jurisdictional issue. The main purpose of this article is to focus on the issue of protecting information privacy and jurisdictional problem through the newly developed cloud computing technology. This article will first introduce the characteristics of cloud computing technology in order to pave the way for further discussion. Then the issue of protecting information privacy and jurisdictional problem will be discussed through disparity of legal protection of information privacy and principles for asserting jurisdiction within Internet. The personal observation and suggestion will be made at the end of this article for a future possible adjustment of infrastructure for the protection of information privacy and jurisdictional decision within cyberspace in order to promote the sense of trustworthiness of the cloud computing technology user.

Keywords: cloud computing, information privacy, information security, legal infrastructure, jurisdiction

1. Introduction

The technology of cloud computing is based on the concept that all the data processing or control will not happen in the end user. This technology is not brand new, but its new application actually arouses a lot of deep concerns that will have profound meaning to our legal infrastructure. The key point for the success of clouding computing technology in terms of application is whether such operation can produce the sense of trustworthiness to its users. Technical measure has always been the fundamental preventive precaution, no matter what kind of aspect in dealing with producing the sense of trustworthiness. Beside the technical measure part, there are two developing issues surrounding the central idea worth notice, which are the protection of information privacy and the jurisdictional issue. The main purpose of this
Creating the Environment for the Prosperity of Cloud Computing Technology (Fa-Chang Cheng)

2. Cloud Computing Technology and its Trustworthy Concern

This section examines the technology of cloud computing and its trustworthy concern.

2.1. Introduction of Cloud Computing

As information and communications technology advances, computing is considered as the 5th most important utility besides water, electricity, gas, and telephony [1]. The success of Internet [2], [3] has led the computing ability shift from a person’s desktop computer to service providers’ computers over the Internet. The service of cloud computing is a trend to deliver, on demand, IT (Information Technology) resources on a pay per use basis. As defined in Buyya et al. [1], “A Cloud is a type of parallel and distributed system consisting of a collection of interconnected and virtualized computers that are dynamically provisioned and presented as one or more unified computing resource(s) based on service-level agreements established through negotiation between the service provider and consumers.” The user data and software reside on the Internet, possibly in data centers and clusters located in different countries, which reduces the role of personal computer to a “dumb terminal” to access cloud via Internet. Computing resources are owned and managed by a cloud service provider (CSP). Using virtualization techniques, these virtualized resources, such as hardware, platforms, or services, are dynamically allocated to scale on demand according to customers’ needs. If a CSP fails to offer the demand, the CSP may outsource to other CSPs.

The working definition of the US National Institute of Standards and Technology (NIST) defined four deployment models of cloud computing - private cloud, community cloud, public cloud, and hybrid cloud. Private cloud is meant solely for an organization, while public cloud is for general public. Community cloud is for specific community composed of several organizations with shared concerns. Hybrid cloud is a composition of clouds. Both private and community clouds are managed by the organization(s) or a third party and may exist on or off premise; public cloud is managed and owned by CSP. There are other different classifications; for example, Ruiter and Warnier [4] classify clouds into public clouds, private external clouds, private internal clouds and hybrid clouds. In a public cloud, the cloud is physically located outside the premises of the organization and the same hardware may host several clouds. In private external clouds, the hardware hosts only one specific customer. This creates better security. In private internal clouds, the infrastructure is managed and owned within the organization. This reduces the security exposure problem of public clouds. Hybrid clouds are a combination of internal and external providers.

NIST also describes cloud computing using three service models - Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS). SaaS provides software applications to users. PaaS provides users with development platforms to develop and execute software. IaaS provides computing, storage, or networking infrastructure.

A comprehensive taxonomy for describing cloud computing architecture is shown in Rimal et al. [5]. The taxonomy is used to survey several existing cloud computing services by comparing features like computing architecture, virtualization management, service, load balancing, fault tolerance, interoperability, storage, security, and programming framework.

The cloud computing has several important benefits. The most appealing one for customers is cost saving. Computing service consumers pay service providers when they access services. They do not need to make a large upfront capital investment in purchasing computers with enough processing power and storage capacity to satisfy the peak demand, thus lowering the barrier to entry for new business. The administration and maintenance costs...
are also reduced, for example, users will no longer need to worry about the problems of hard drive crashing, backups, or upgrading. Since the computing and storage facilities are in the cloud, users can use simpler devices, like less powerful computers, cell phones, or PDAs (Personal Digital Assistants), to access the cloud, and they can access from anywhere in the world where they can connect to the Internet, which provides mobility and convenience.

Cloud computing service providers are relieved of the piracy problem of unauthorized copying, which has plagued the software developers for years. Since the computation occurs on providers’ servers, it will be extremely difficult for copying or reverse engineering. The intellectual property protection is thus easier. Besides, cloud computing service providers can be always sure that their customers are using the most up-to-date version of their software. Finally, they can use sophisticated data mining algorithms based on customers’ data and serve carefully targeted advertising to customers.

2.2. Trustworthy Concern

The advantages of cloud computing can become disadvantages. Although the cloud providers can afford and might implement better security mechanism into their systems than the common end-users, like hiring security experts and installing anti-virus software, the facts of remote access, virtualization, platform sharing, border crossing, lack of data control, and massive use of third party services and infrastructures all make the trustworthy of cloud computing technology a major worry. A complete list of risks can be found in Catteddu and Hogben [6], where the European Network and Information Security Agency (ENISA) has identified 35 risks of using cloud computing.

Firstly, clouds are on Internet; therefore, all the security problems related to Internet, including frauds and attacks by hackers, may happen. Actually the problems become more significant because cloud services make heavy use of Internet. Secondly, sensitive data, like medical records, are no longer protected by physical quarantine. Ristenpart et al. [7] argue that fundamental risks arise from sharing physical infrastructure between users, even when their actions are isolated through machine virtualization as within a third-party cloud compute service. Thirdly, data may be stored and processed in different geographical locations with different regulations. Users may lack awareness regarding the location, which will cause serious jurisdiction and legal compliance troubles. Fourthly, CSPs may hesitate to provide a safer mechanism because of business considerations. For example, Soghoian [8] believes that the likely reason Google took several years to offer HTTPS (Hypertext Transfer Protocol Secure), an industry standard encryption protocol, by default is the issue of cost because encryption takes processing power and memory. According to Kant et al. [9], the computational cost of the transactions using SSL (Secure Socket Layer) will increase by a factor of 5-7. In addition, for those companies with business models getting profit from data mining and then serving advertising, they definitely won’t be happy to see their customers upload encrypted data, which obstruct the data mining job. Fifthly, some people are worried because it will be easier for government snooping [8]. Government may force CSPs to place a back door. Soghoian [8] mentioned that some key features, like identifiable customers, automatic, silent updates, and the complete absence of visible product releases, make it far easier for the government to effectively force the deployment of covert back doors on clouds than traditional software products. In sum, from technical point of view, the cloud computing technology really raises the trustworthy concern in its application.

Several technical solutions have been proposed for the security and privacy problem. The most obvious way out for users is to encrypt whatever data they are going to put in the cloud. But it will increase the cost of computation and it is technically cumbersome to process the data in an encrypted form. For example, searching and indexing the data become a challenging job. Plainly download all the encrypted data, decrypt and search on local computers is not practical. Thus, a fully homomorphic cryptosystem, a system which can perform calculations, basically addition and multiplication, on encrypted data without decrypting and still keep them secure has long been a desire. Recently, an amazing work of fully homomorphic encryption using ideal lattices [10] has been announced by IBM. Unfortunately, it still takes time to become practical. As Gentry, the author of fully homomorphic encryption using ideal lattices, estimates, in the case of performing a Google search with encrypted keywords, for instance, it would multiply the necessary computing time by around 1 trillion. It probably takes 40 years to be as efficient as a search today according to Moore’s law estimated by Schneier [11].
Therefore, a practical fully homomorphic cryptosystem is still an open issue. Several other approaches also have been presented. Chow et al. [12] propose to extend control measures from the enterprise into the cloud through the use of Trusted Computing and applied cryptographic techniques. A privacy manager is suggested by Pearson and Shen [13]. And PasS (Privacy as a Service), a set of security protocols for ensuring the privacy and legal compliance, is used to maximize users’ control in Itani et al. [14]. Besides, some studies focus on auditing or assessment. For example, to check the integrity of data on clouds, it is necessary to introduce a third party auditor. Wang et al. [15] present a privacy-preserving public auditing system for cloud data storage security by utilizing a public key-based homomorphic authenticator and integrating it with random mask technique while keeping the requirements of auditing the cloud data storage without demanding the local copy of data, introducing no additional on-line burden to the cloud user, and bringing in no new vulnerabilities toward user data privacy. All these measures mentioned here are aiming for the purpose to enhance the trustworthiness of cloud computing technology.

3. Information Privacy Protection within Internet as an Approach to Enhance the Trustworthiness of Cloud Computing Technology

Although the newly developed cloud computing technology may have influenced the rights of both business entities and individuals, it is not the authors’ intent to discuss the protection of legal rights pertaining to business entities, such as the issue of unfair competition, the protection of trade secrets etc. The thinking behind this differential treatment to the legal issues with regard to such cloud computing technology is based upon not only those business entities that have the predominate financial power to stand for their own rights but also, in unfair competition litigation between business entities, the rule of reason moves the judgment for unfair competition toward case-by-case decision-making process and it is still unclear what the balancing result for such cloud computing would be until the real case comes out. The above-mentioned situations for business entities actually elicit the idea that individuals are in a disadvantageous position and need clear legislation for the protection of information privacy while facing the new development of cloud computing technology. In the following discussion, focusing on the protection of information privacy within cyberspace, this paper will first briefly introduce the current status of information privacy protection in the United States and European Community within cyberspace, and then also discuss the potential problems for these two different legal approaches when trying to regulate activities based upon the newly developed cloud computing technology. The experience of Taiwan while facing the revision of Personal Information Protection Act will lead to the discussion of the future prospective and best solution for the impact of such technology to legal protection in individual information privacy at the end of this article.

4. The Substance, the Potential Problems and the Thinking of Future Prospect for the Protection of Information Privacy within Cyberspace, also with Taiwan’s Experience

There are two different level of question need to be inquired for understanding the substance of information privacy. The first level of discussion is whether the specific circumstances warrant the protection of information privacy. The second level concerns the legal interests of information privacy in balance with other interests and the type of protection that is appropriate if the answer to the first level of discussion is positive.

4.1. The Line for the Protection of Information Privacy in the United States

In the United States, it could be fairly said there are different laws that can be used in protecting information privacy within cyberspace. It is not the intention of this paper to discuss individual legislations in detail. This legislative phenomenon indicates that information privacy is treated differently according to different kinds of information or entities. It also shows that one kind of information privacy may have different laws regulated at the same time. It is still not very clear about the position of information privacy in constitutional hierarchy; at least, the Supreme Court never admits the information privacy as the fundamental right. Even information privacy is treated differently in cyberspace according to different kinds of information or entities as mentioned before; the general tendency is the preventive measurements (standard of
information security and notification of such security breach) will be imputed on such protection of information privacy in cyberspace. And it is also worth noticing that there has been some insufficiency apparently in the protection of information privacy within cyberspace in the United States.

4.2. The Line for the Protection of Information Privacy in the European Community

In the European Community, the most important Directive for the protection of individual information privacy is 95/46/EC. In Directive 95/46/EC, there are several aspects in the issue of protecting individual information privacy which need attention. First of all, Article 8 of Directive 95/46/EC manifests that personal data that reveal racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership and data concerning health or sex must be protected with certain exceptions. And also in Directive 2002/58/EC on privacy and electronic communications, the notification of information security breach is also required for providers of public electronic communications networks and services including telecom operators, mobile phone communication service providers, internet access providers, providers of the transmission of digital TV content, and other providers of electronic communication services that are offered to the public instead of private electronic communications networks and services (closed user groups and corporate networks). Any breach of information security must be reported to the authorities, and if it is likely to adversely affect any individual, and then notify that individual. Besides the scope of protection of information privacy and the notification of information security breach, in Article 10-11 of Directive 95/46/EC, the notification of information collection is generally required except for some exceptions, which is different from focusing on specific types of information in the United States. From the above-mentioned statement, it can be fairly said the scope of information privacy protected in European Community and the requirement of notifying information collection are broader (intensive) than in the United States, and in the European Community, the burden of notifying information security breach is imputed on the communication service provider rather than the data processing entity.

One might be arguing that the protection of information privacy in cyberspace in the European Community seems stronger than in the United States. This is reflected both in 95/46/EC and the safe harbor agreement between the European Community and the United States. According to Article 25 of 95/46/EC, the member states basically can transfer the personal data outside the European Community only if such third country has adequate protection of personal information. To follow the requirements contained in the safe harbor agreement is equal to satisfy the meaning of adequate protection of personal information. The transferee must be certified by Federal Trade Commission and register with the Department of Commerce by disclosing its privacy policy [4] in order to qualify the trans-border information requirement in Article 25 of 95/46/EC.

4.3. The Fundamental Difference between these two Lines and Specific Concerns for the Protection of Information Privacy related to Cloud Computing Technology both in the United States and European Community

There is some fundamental difference between these two lines of thoughts concerning the protection of information privacy. The European Community line of thoughts considers the legal interest of information privacy to be a fundamental human right. The United States line of thoughts regards the protection of information privacy on a case-by-case basis, which means that the legal interest is not a fundamental human right [16]. If the legal interest of information privacy is a fundamental human right, like the situation in most European countries, the “reasonable expectation” should be broader, the balance of interests should be easier and the protection infrastructure of information privacy should be more restrictive than if information privacy is not seen as a fundamental human right, like the situation in the United States.

Beside the different approaches adopted by the United States and European Community, the specific difficulties in applying the newly developed cloud computing technology to current protection of information privacy in cyberspace for both the United States and the European Community will be pointed out in this section to indicate possible confusions existing in these two jurisdictions.

In the United States, there are problems in applying the protection information privacy to such newly developed information technology. For example, in “The Stored Communications
Act”, except E-mail which may be qualified as the electronic communication service, to be the remote computing service, the service must be “solely for the purpose of providing storage or computer processing services”. These definitions may leave multi-functioned cloud computing services outside the regulation of “The Stored Communications Act”, although this does not seem to be the intention of legislators who have passed the law [17]. Also in HIPAA or even American Recovery and Reinvestment Act of 2009 enforced the protection of on-line medical information privacy, whether the meaning of statutory entities or their business associate includes different kinds of cloud computing service providers needs to be clarified to make sure such service providers are regulated by these two legislations. There are also problems in deciding whether the cloud computing service providers are the data controllers or the data processors where the former is mainly regulated in the European Community, especially if the cloud computing service provider may function as both, a data controller and data processor [18].

4.4. The Personal Information Protection Act in Taiwan and the Overhaul for the Challenge to Protect Information Privacy within Cloud Computing Environments

From the description of legislations and potential problems for both the United States and European Community in facing the issue of protection of information privacy within cloud computing environments, it can be seen that there are different approaches and also different potential problems in protecting information privacy within the application of cloud computing technology. Taiwan also cannot immune form facing this kind of situation. The discussion in this section will introduce newly passed Personal Information Protection Act and its problems in reality, especially facing the cloud computing technology. And the suggestion will be brought up especially through the discussion of Taiwan’s experience.

4.4.1. The Personal Information Protection Act in Taiwan and its Social Response

In Taiwan, the legislators passed the revision of Computer-Processed Personal Data Protection Law in 2010 which is entitled “Personal Information Protection Act”. The basic blue print for Personal Information Protection Act for protection of personal information is formed on the lines of the counterpart protection in European Community with some more protection to the degree.

The observation of the Personal Information Protection Act in Taiwan to the development of cloud computing technology is the Act not only causes the confusion and difficulty with this regard but sometimes even makes the operation of cloud computing technology impossible. First, the major confusion will result from the legal hierarchy related to other civil or criminal laws which can also be used as the channel to protect the information privacy. According to the legislative explanation, the Personal Information Protection Act shall be subordinate to other civil or criminal laws if they are directly conflicting with each other. As known from the introduction just mentioned before, the Act is more stringent in protecting the information privacy, but unfortunately, it is at the bottom of legal hierarchy in protecting the information privacy. There is a highly possibility that the disparity of protection (balance of interest) would come out at the same situation just because based on the different legal authorities.

Secondly, the highly regulated provisions in the Act (for example the notification of acquiring information and its retroactive effects) really cause a lot of panic in Taiwan. That is exactly why the Personal Information Protection Act is still waiting for its effectiveness date even the Act has already been passed by the legislation in Taiwan. How to exactly regulate the personal information pertained in the cloud computing technology is still up in the air.

Finally, some provisions in the Act will actually make the operation of cloud computing technology almost impossible. For example, under the Article 6 of the Act, the sensitive personal information cannot be gathered even it is consented by the resource person except for the listed specific purpose. Under the provision, it is highly unlikely to use the cloud computing technology in personnel health information gathering. It is also highly questionable for Taiwan to establish the general public health information cloud without the specific purpose for medical treatment, personal hygiene or prevention of crime.

4.4.2 The Overhaul of Protection in Information Privacy

After explaining the possible difficulties to apply the current legislations to regulate the
newly developed cloud computing technology, especially based on Taiwan’s experience, to bring the discussion up to the next level is to inquire how to overhaul the protective infrastructure for the information privacy in order to enhance the sense of trustworthiness to its users. This article will divide the protective infrastructure for the information privacy into two parts: the substantive legislation and the accountability practice.

First, to the substantive legislation part, besides clarifying the legal definitions or confusion in the legislation among the United States, European Community and Taiwan as mentioned before, one important task needs to be tackled is whether these current legislations among these jurisdictions over-excessively or insufficiently protect the information privacy under the clouding computing technology which needed to make the change. There is no doubt that the development of cloud computing technology highly raised the concern about information privacy within cyberspace and the heavy use of such service is the reason why the privacy concern becomes so significant. So, at first, it is suggested that at least the strength of information privacy protection under this cloud computing technology shall not lower than the general protection of information privacy. As to whether to choose the United States approach or European Community approach is the issue that needs to be discussed. It is observed that the fundamental reason for these two kinds of differential treatment is different recognitions of information privacy in constitutional hierarchy. It is suggested that the notification of information security breach and informed consent should be regulated as a preventive measurement; not only is it a common trend both in the United States and the European Community but also is focused on the third-party unlawful activity and self-determination without serious issues of balance of interests. With regard to the notification of acquiring information and other possible legal remedies, it is better to adopt the United States approach which is more flexible in balancing different interests in the protection of information privacy.

As to the accountability practice part, if the substantive legislation is the core of protecting information privacy within cyberspace then the concept of accountability is the system operator. The concept of accountability, which is first established by the Organization for Economic Co-operation and Development ("OECD"), provides an improved solution to trans-border data protection. Five essential elements of accountability, according to OECD, include 
(i) Organization commitment to accountability and adoption of internal policies consistent with external criteria;
(ii) Mechanisms to put privacy policies into effect, including tools, training and education;
(iii) Systems for internal, ongoing oversight and assurance reviews and external verification;
(iv) Transparency and mechanisms for individual participation; and
(v) Means for remediation and external enforcement.

The phenomenon of paying attention not only to the substantive legislation but also to the accountability practice is really happening in Taiwan. The Science & Technology Law Institute under the Institute for Information Industry in Taiwan is now trying to realize the accountability concept through building up the certificate system in protecting the personal information privacy, especially for the purpose of protection within Cyberspace. Through building up the system to make entity to commitment to legal compliance through technology measurement, there are three different organizations with their own function for the system operation: the organization to set up the standard which is the Science & Technology Law Institute, the organization to certify the fulfillment of the standard and the organization to counsel the implement of the system. The newly development in Taiwan is in its beginning stage, and the trend of emphasizing the accountability practice is worth continuing attention and observation. Even though the principle of accountability is the important part to the protection of information privacy within cyberspace, this article suggests that there are some concerns with establishing such a certificate, especially in Taiwan. Judicial practices to interpret the “Personal Data Protection Act” in Taiwan are still lacking. Differences in the protections within other states’ jurisdictions also must be overcome in implementing the system, especially if the infringement of information privacy occurs within cyberspace. Therefore, this article would like to make two suggestions for such certificate system: to establish slightly different standards suitable for different types of situations in the protection of information privacy and to review the status quo periodically to balance it with the judicial reality.
5. Jurisdictional Decisions within Cyberspace to the Trustworthiness of Cloud Computing Technology

As said in the beginning of this article, the jurisdiction issue within cyberspace is the other developing issue in terms of promoting the trustworthiness to the cloud computing technology. Unlike the protection of information privacy, there are several considering interests constantly surrounding the issue of jurisdiction: the interests of defendant, the state sovereignty for criminal investigation and the interests of plaintiff. Since the consideration in state sovereignty for criminal investigation is unique to decide the criminal jurisdiction, therefore, the following discussion will generally divide into three aspects: the special characters in asserting jurisdiction within cyberspace, the civil jurisdiction and the criminal jurisdiction.

5.1. The Special Characters in Asserting Jurisdiction within Cyberspace

Whenever a court wants to try a case, there should be a jurisdiction behind such a court as procedural justification to hear the case. Traditionally, different sovereignties have their own rules to establish jurisdiction and these rules can be categorized under several types of scenario. In the information age, because of the trans-border character of Cyberspace activities, it is common to encounter the complex legal issue to decide whether the sovereignty has the jurisdictional reach in this fictitious environment. The most controversial situation in the issue of Cyberspace jurisdiction is to bring in the out-of-state defendant into the jurisdiction to receive a trial or to enforce a foreign judgment based upon such jurisdiction. Especially when different sovereignties may have different kinds of attitudes towards the same issue, the jurisdictional dispute will usually conclude the winning or losing of the case. The best example is the Yahoo case. In this case, two organizations sue Yahoo! Inc. for violating the French law against auctioning Nazi objects in the French court. Even Yahoo claimed that its targeted customers were in the United States, not France, and prohibiting the auction of Nazi objects violated the protection of freedom of speech in the United States; the French judge thought interested French customers could still access the website and the advertising banner in French indicated that Yahoo was “targeting” the French users. Therefore, the judge thought the French court had jurisdiction over this dispute. After they successfully won the case in the French court, they tried to enforce the final judgment in the United States. The District Court of California in the United States regarded not only the enforcement of such judgment would unduly hamper the protection of freedom of speech in the United States but that such contact in that case was insufficient for the French court to assert jurisdiction over the issue here. So, the court in the United States cannot enforcement the French judgment [19].

The purpose of mentioning this case is to show how important and unpredictable it is in expending the assertion of jurisdiction outside the sovereignty territory within Cyberspace. In other words, the issue would be how to establish a personal jurisdiction, instead of in rem jurisdiction, related to an out-of-state defendant. This is the most jurisdictional situation that occurred within the Cyberspace because of the trans-border characteristics of Cyberspace. Beside, the Internet is designed to follow an end-to-end principle, an approach of putting intelligence at the end nodes of the network while letting the networks just deliver the bits without caring what the data is or what the users are doing. Following the layered approach of network design (application, transport, network, link, and physical layers), anyone can create new applications and run them over the Internet without worrying about how the bottom layers work. So, tracing the source of the attacks, or intentional or negligent behavior is difficult especially when most of the time communications take place across the border. Without the cooperation of other jurisdictions, it is difficult for one jurisdiction to get evidence to prove the case.

The fictitious two-way trans-border and hard-tracing characteristics of Internet have made it quite a challenge than ever to apply the rule of law for jurisdiction either technically or theoretically and the issue of jurisdiction with cyberspace is unpredictable more than ever, hurting the trustworthiness in a sense.

5.2. The Current Principles for Civil Jurisdiction

There are several possible judicial solutions developed by legislations or legal principles (constitutional requirements) followed by courts while they are facing the cyberspace jurisdictional issue of bringing the out-of-state defendant before justice in a civil litigation. The first possible solution introduced in this article emerged from a 1997 federal case in the United
States named “Zippo” (Zippo Manufacturing Co. v. Zippo Dot Com, Inc. 1997; 953 F. Supp 1119.), In this case, the court brought forward a “sliding scale” theory to decide whether to assert jurisdiction over the website in a contract dispute case established outside the state. Because in the United States, the constitutional requirement for asserting jurisdiction over the out-of-state defendant in a civil litigation is the “minimum contact” of such defendant with general consideration of “fair play and substantial justice”, especially when the state court trying to expend jurisdiction to the out-of-state defendant based upon long-arm jurisdiction contained in states’ constitution [20]. It means that the defendant must purposely avail himself or herself of the benefits in the forum state with the consideration of the justice before asserting jurisdiction to such out-of-state defendant [21].

According to the “sliding scale” theory, there are three possible types of contact for website to the defendant in a contract dispute case: active contact, passive contact, and interactive contact. The active contact of the website means it really comes to a contract with the plaintiff in case. This kind of contact is sufficient to constitute the “minimum contact”. On the contrary, only passive contact of the website which only provides information to the potential customer is insufficient to constitute the requirement of “minimum contact”. As to the interactive contact, the quality of interactivity will decide whether it satisfies the “minimum contact” requirement. This idea of using technology characteristics to serve as the judgmental criteria is also borrowed in the defamatory case. According to the statement just mentioned, if the defaming website is passive in characteristic, the possible outcome for jurisdictional issue of such defamation allegation would be that there is no jurisdiction over such out-of-state defendant. Using this kind of jurisdiction methodology within cyberspace was seriously criticized by the commentator because the passive character does not necessarily mean that the defendant does not purposely avail himself (herself or even itself) of the benefits of the forum state, especially in defamatory litigation, the lack of explicit intent to defame the plaintiff in a given case is difficult to be decided by the passive characteristic of the defendant [22]. This thinking behind the criticism gradually leads to the development of targeting theory which means that the defendant was targeting the jurisdiction in issue or the plaintiff (Revell v. Lidov. 317 F.3d 467 [5th Cir. 2002]). In the targeting theory, the intent of the defendant will substitute for the technical mechanism in order to accord with the “minimum contact” plus “fair play and substantial justice” requirement under the Constitution in the United States and the decision of intent is primarily facts originated.

The second possible solution for asserting jurisdiction within cyberspace is probably hinged upon the general agreements in some regional trans-border treaties. Especially in the European Community, the principles for jurisdictional decisions are divided by types of activities within cyberspace through regional trans-border agreements. For example, the Brussels Regulation developed from the Brussels Convention is regulating the issue of how to decide the assertion of jurisdiction within Cyberspace related to business-to-customer (B2C) situations. Not only the Brussels Convention treats the jurisdiction issue differently between the consumer contract and the commercial contract, but the following Brussels Regulation is more favorable to the consumer than the Brussels Convention in the issue of cyberspace jurisdiction. Generally speaking, in an ordinary commercial contract, the appropriate jurisdiction to file a lawsuit is either the place of performance of the obligation in issue or the place where the transaction is (should have been) completed. Under the Brussels Regulation, the consumer in a consumer commercial transaction within cyberspace will have the choice bringing the legal litigation against the commercial business in the jurisdiction of his (or her) domicile as long as the website is interactive in its characteristic. The meaning for interactivity seems to be a threshold easy to be satisfied, for example having a language choice function in a website can mean it is interactive. Any consumer commercial contract made through an interactive website means that the business is directing its activities to the consumer’s state per se and the consumer has the right to file the lawsuit in his (her) home state. And furthermore, in Brussels Regulation, the contractual agreement between parties cannot limit the consumer’s rights to choose his (or her) domicile as the trial venue unless such mutual agreement is formed after the contractual dispute arises. The implication behind the jurisdictional approach in the European Community in this regard is that the idea of social warfare to protect the consumer is more predominant in the European Community than in the United States. Such legislative philosophy is distinctive of the targeting theory resulting from the constitutional requirements of both minimum contact and fair play with substantial justice. From the above-mentioned discussion, it can be fairly stated that different sovereignties have their rules to bring out-of-state defendants to justice. In the following
discussion and explanation, two suggestions are given. One suggestion is that commercial transaction of small amounts should use ODR (on-line dispute resolution) in dealing with jurisdictional issues. The other suggestion is the targeting theory would be the best choice for asserting civil jurisdiction.

First, it has been said that ODR (on-line dispute resolution) is the cost-effective and convenient way to deal with contractual disputes between parties [23]. Under the ODR structure, there is no need for the state sovereignty to intervene a contractual dispute between parties by asserting jurisdiction. Parties will work out their dispute through some kind of on-line dispute mechanism. From the above-mentioned statement, even if the application of ODR seems better than judicial intervention in the legal issue rising out of cyberspace, there are some serious concerns pertaining to such mechanism. Some commentator worried about the unbalance of bargaining power between the parties, which could lead to ODR injustice. The most important concern is which people have the problem to trust this ODR mechanism will cause its total failure [24]. For the purpose of easing those concerns, this article will take the stand that ODR will only be used in commercial transactions involving small amounts.

Secondly, the targeting theory is still the best choice from the predictable point of view since the plaintiff needs to prove the strong intention of defendant entering into such jurisdiction. This paper would also argue at the same time in this article that, by adopting targeting theory, the dilemma between getting the evidence and asserting the jurisdiction within cyberspace could be alleviated because to satisfy the proof of defendant “targeting” sometimes means the evidence has been sufficient enough in a sense.

5.3. The Assertion of Criminal Jurisdiction with its Predictability

There have been several theories using by nations for deciding the jurisdiction issue in criminal cases [25]. The first theory is called “territoriality” principle. Under this theory, the nation where the crime committed, either based on the conduct point of view or the result point of view, has the jurisdiction. The second theory for criminal jurisdiction is “nationality” theory. In this theory, it doesn’t matter where the crime committed to assert the jurisdiction, what matters is the perpetrator’s nationality. And the last theory for criminal jurisdiction is named “universality” principle. This theory is generally used in some specific high-profile crime, for example the war crime, genocide etc. The observation for the real world in asserting jurisdiction within Cyberspace is that the “territoriality” principle is dominated with certain specific situation by adopting the “nationality” theory in order to the victim citizen.

In Taiwan, generally speaking, the traditional jurisdiction assertion in criminal cases is based upon the “territoriality” principle according to the general criminal code. There is one thing worth noticing that the interpretation of “where the crime committed” will definitely affect the imputation of asserting jurisdiction. Based on author’s personal observation, compared with the court in the United States, the court in Taiwan seems reluctant to assert jurisdiction within cyberspace just because there would be some criminal effects influencing the territory. Moreover, the trans-bordering and hard-to-trace characteristics to Cyberspace Criminal investigation often times impede the substantial power of court to assert jurisdiction because lack of solid digital evidence. And unfortunately, the judicial system in Taiwan doesn’t get sufficient investigative information from other jurisdictions. In order to alleviate the practical predicament, the government in Taiwan is attempting to require the telecommunication carriers in Taiwan to set up gateways in case of possible criminal investigation through legislative or administrative process. This measurement would make the law enforcement in Taiwan easier to gather digital evidence within the territory.

To sum up the experience in Taiwan about how to reach the balance between the assertion of jurisdiction indicating sovereignty and the practicability of investigation in a cyberspace crime for the law enforcement, to set up gateways within the territory is the concrete solution for asserting jurisdiction based on the “territoriality” principle, also increasing the predictability at the same time. Other than the situation mentioned here, the law enforcement is going to fall into an uncertain and dicey position in asserting jurisdiction which is pending on the circumstances.
6. Conclusion

The fundamental idea for the cloud computing technology to be prosperous is the trustworthiness of such technology. This article reviews two important but still developing issues, the protection of information privacy and jurisdiction assertion respectively, as two different measures to promote the trustworthiness of the cloud computing technology. In the issue of protecting information privacy, the study in this article concludes that preventive approaches (informed consent, notice of security breach or even technical design) are practical and trendy to achieve the goal of promoting trustworthiness. And this study also stands the point that the more flexible approach should be adopted in case of defining information privacy and balancing the interests of protecting information privacy with other conflicting interests because of the evolution and development of clouding computing technology. The concept of accountability will also jump into the scenario serving as the system operator for the protection of information privacy beside the substantive content of protection. In the issue of jurisdictional decisions, the civil jurisdiction is going to emphasize on the defendant’s intent to target the jurisdiction in case because in considering of the unduly burden to the defendant but the criminal jurisdiction shall add more emphasis on the integrity of state sovereignty. The predictability and state’s willingness for the assertion of jurisdiction within cyberspace will definitely increase the sense of trustworthiness of cloud computing technology. The cloud computing technology would not be able to get on its feet without the proper social environment to foster the sense of trustworthiness and which is the purpose of this article to promote the idea looking forward seeing the bright future for the prevalence of cloud computing technology.

References


