Cyberlaw

A Speech at Hang Zhou University of Commerce and Technology

September 2004
Takato Natsui
Professor, Meiji University Faculty of Law

1. Introduction

My book “電子署名法” [The electronic signature law] will be recently published in Chinese with the support of some wonderful friends and colleagues in China. To have my book published in Chinese is a tremendous honor. I would like to take this opportunity to express my deepest gratitude and appreciation to everyone who cooperated with the Chinese translation.

I was asked by my Chinese colleagues if I would give a lecture at Hangzhou University of Commerce and Technology to mark the publication of the Chinese version of my book. I was deeply honored and gladly accepted.

China and Japan have had close ties since ancient times. Japanese archeologists believe that China and Japan have had close cultural and industrial relations for at least 2000 years. There are references to Japan in ancient Chinese history texts such as 魏志倭人伝 [Wei Chih] and 漢書東夷伝 [Han History].

During their long history, there have been periods when China and Japan had friendly relations, and other period when their relations were not so fortunate. Throughout this extremely long period of exchange, however, numerous aspects of Chinese culture and systems merged into Japanese culture and social organizations. Confucianism, Taoism, and Buddhism were all conveyed to Japan from China. Many other aspects of culture were also brought from China including wood building construction, ceramics, music, and calligraphy, to name just a few. Some of these items made their way to Japan via Korea, while other came directly from China.

While in high school and university, I studied extensively about Chinese philosophy, arts, and history from the 殷 [Yin] and 周 [Zhou] Dynasties right up to the People's Republic of China. Among the innumerable notable persons who appear in Chinese history, I particularly admire 顔眞卿 [Yan Zhenqing] (709-785) of the 唐 [Tang] Dynasty and 岳飛 [Yo Fei] (1103-1141) of the 宋 [Song] Dynasty. These two military commanders are renowned for their calligraphy and are known as wonderful educators. When I was in school, I studied ”文武両道” [scholarship and the martial arts] and “君子和而不流” [The gentleman is friendly but not easy to delude into following other people.]. 顔眞卿 [Yan Zhenqing] and 岳飛 [Yo Fei] were truly great men who embodied “文武両道” [scholarship and the martial arts]. “君子和而不流” [The gentleman is friendly but not easy to delude into following other people.] is a term found in the 中庸章句 [Doctrine of the Mean] by 朱子 [Chu His], a true expert on

ancient texts, and has the same meaning as the phrase ”君子和而不同” [The gentleman is friendly but a person of principle.] found in 論語 [The Analects of Confucius]. Confucianism as a fundamental state policy was clearly rejected in China and Japan during certain periods. Nonetheless, I believe that the words and life philosophies of great historical persons are still worthy of study even today. In today's modern society, as international exchanges become ever more common and relations between states becoming close, leaders in every field must have a strong sense of a spirit of “君子和而不流” [The gentleman is friendly but not easy to delude into following other people.]. In other words, in modern society, be it in China or Japan, we must maintain a strong sense of pride in our own ethnicity and culture even as we seek friendly and harmonious international relations. Modern society demands that all individuals address this type of extremely difficult issue. As expressed by 論語 [The Analects of Confucius] and ”温故知新” [an attempt to discover new things (truths) by studying the past through scrutiny of the old], during its long history, China has confronted innumerable complex foreign relations issues. And we can learn much by studying them. In this way, I personally have absorbed much of Chinese culture and philosophy.

I have had the opportunity to participate in numerous conferences concerning cyber law in various cities and at many different universities around the world. My first visit to China however, is to Hangzhou. Hangzhou has extremely close ties to 顔眞卿 [Yan Zhenqing], 岳飛 [Yo Fei], and 朱子 [Chu His]. For this reason, I am deeply moved that my first visit to China is to Hangzhou.

2. Structural Changes in the Modern World

Modern society is founded on information networks such as the Internet. It goes without saying that in modern too, it is living people who engage in day-to-day activities, labor, and perform various works. The vast majority of our lives are completely unrelated to network technology. Individuals form close ties of affection with each other. Familial bonds too mean nothing without emotional ties. In shops, transactions are conducted between shopkeepers and customers. Many of the problems that occur in society arise because of intertwining human relationships. In addition, it is the job of the police to catch criminals, and the job of the courts to punish them.

In modern society, however, an extremely large number of jobs make use of information network technologies applied to computer systems. As a result, it is possible for people who live at extreme distances to perform a variety of jobs. There are numerous Chinese companies that use information networks to engage in business globally. Even in fields such as animation and film, many Chinese companies, like companies in Japan and South Korea, have come to use computer image processing extensively, and they are advancing into markets throughout the world.

In a society based on information networks in such a manner, it is important that we take incidents from the past as lessons. In China and in Japan, we have to consider

together the solutions to common problems. For example, in a network-based society, it goes without saying that the physical structures of information networks must be made secure. At the same time, it is also necessary to establish and implement properly the legal structures to ensure that transactions conducted using information networks are carried our safely. When the reliability of transactions using information networks cannot be ensured, economic development cannot be hoped for, and the results of everything that has already been accomplished will be for nothing.

The legal structures that are used to ensure the safety of information networks are quite diverse. Criminal statutes to punish persons who gain improper access to information systems, who cause damage such systems, and who commit fraud are necessary. It is also important to reconsider basic laws such as the Civil Code and the Commercial Code from the perspective of international coordination among the various laws that govern transactions. This is true for both China and Japan. Also necessary are legal systems to protect the electronic structures that safeguard transactions using information networks and to establish that the parties to transactions are really who they say they are. The Electronic Signature Law may very well be the most important single element within that legal structure.

Today in Japan, in addition to electronic signatures used by private companies as specified in the Electronic Signature Law, there is also an electronic notary system operated by public notaries and a public identification certification service operated by local governments. As these systems were instituted after publication of my book, it does not discuss electronic signatures or the electronic certification system in Japan. It does, however, explain the fundamentals and the ideas behind electronic signatures and electronic certification systems, and it has been read by many people in Japan. Even today, it continues to be read by many people. In order to show the importance of the Electronic Signature Law, the book also explains the uniqueness of legal incidents that can occur in cyberspace and comments on the Japanese Civil Code and other statutes that regulate business transactions. Consequently, I believe that this book can be of considerable reference value to legal scholars, entrepreneurs, and students who wish to learn about transactions based in information networks and the legal systems around the world that regulate them.

As the author of this book, I would be greatly honored and pleased if it could assist in China's secure and steady economic development and contribute to the growth of friendly relations between China and Japan.

I will be discussing on the unique characteristics of the cyber world and on the various legal issues that can arise in there.

3 What is Cyberspace?

The word “cyber” most likely came into widespread use starting in the United

States during the 1940s when Norbert Weiner and his colleagues developed the idea of cybernetics. Weiner referred to the existence of a feedback function as an internal function regardless of whether it is possessed by a living organism or an inanimate object as "cybernetics." This term is the origin of other words such as "cyborg" and "cyberspace."

The American author William Gibson wrote a number of science fiction novels in the 1980s that take place in cyberspace. The most famous of his novels is Neuromancer. After a number of Gibson's novels attracted considerable attention, it become not only trendy to refer to the space on information networks such as the Internet as cyberspace, but went on to become commonplace.

Cyberspace is sometimes explained as a "virtual space." Although it is virtual, this does not mean that cyberspace does not exist.

A key point in comprehending cyberspace and the various conflicts that can occur in cyberspace is due to understand that cyberspace is not imaginary, but is a part of reality.

The Internet is a representative example of cyberspace. It is true that the Internet is no more than a collection of electronic signals. It appears that the Internet exists on your monitor. The Internet, however, is not imaginary and is an actual part of reality.

4 Cybercrime

It almost goes without saying that crime also takes places in cyberspace. Some typical examples are unauthorized access to others' computer systems and Internet fraud. These types of crimes are referred to as cybercrimes.

Cybercrime is not a type of crime that affects only certain people in certain countries. Cybercrime can occur anywhere in the world where it is possible to access information networks such as the Internet, and anyone, located anywhere, can become a victim of cybercrime.

As a result, many countries around the world are promoting international measures to deal appropriately with cybercrime. The European Union Convention on Cybercrime is a typical example. Countries that are not members of the EU are also seeking to ratify this Convention, and Japan is taking the measures necessary to acceded to it.

The Convention on Cybercrime (ETS 185)1 provides that the following are the types of crimes concerning which the laws of different countries should be coordinated. These are considered the most serious cybercrimes.

> Article 2 – Illegal access
>
> Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally,

[1] http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm

the access to the whole or any part of a computer system without right. A Party may require that the offence be committed by infringing security measures, with the intent of obtaining computer data or other dishonest intent, or in relation to a computer system that is connected to another computer system.

Article 3 – Illegal interception

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the interception without right, made by technical means, of non-public transmissions of computer data to, from or within a computer system, including electromagnetic emissions from a computer system carrying such computer data. A Party may require that the offence be committed with dishonest intent, or in relation to a computer system that is connected to another computer system.

Article 4 – Data interference

1. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the damaging, deletion, deterioration, alteration or suppression of computer data without right.
2. A Party may reserve the right to require that the conduct described in paragraph 1 result in serious harm.

Article 5 – System interference

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the serious hindering without right of the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data.

Article 6 – Misuse of devices

1. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right:
a. the production, sale, procurement for use, import, distribution or otherwise making available of:
   i. a device, including a computer program, designed or adapted primarily for the purpose of committing any of the offences established in accordance with Article 2 – 5;
   ii. a computer password, access code, or similar data by which the whole or any part of a computer system is capable of being accessed

with intent that it be used for the purpose of committing any of the offences established in Articles 2 - 5; and

b. the possession of an item referred to in paragraphs (a)(1) or (2) above, with intent that it be used for the purpose of committing any of the offences established in Articles 2 – 5. A Party may require by law that a number of such items be possessed before criminal liability attaches.

2. This article shall not be interpreted as imposing criminal liability where the production, sale, procurement for use, import, distribution or otherwise making available or possession referred to in paragraph 1 of this Article is not for the purpose of committing an offence established in accordance with articles 2 through 5 of this Convention, such as for the authorized testing or protection of a computer system.

3. Each Party may reserve the right not to apply paragraph 1 of this Article, provided that the reservation does not concern the sale, distribution or otherwise making available of the items referred to in paragraph 1 (a) (2).

Article 7 – Computer-related forgery

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the input, alteration, deletion, or suppression of computer data, resulting in inauthentic data with the intent that it be considered or acted upon for legal purposes as if it were authentic, regardless whether or not the data is directly readable and intelligible. A Party may require an intent to defraud, or similar dishonest intent, before criminal liability attaches.

Article 8 – Computer-related fraud

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the causing of a loss of property to another by:

a. any input, alteration, deletion or suppression of computer data,

b. any interference with the functioning of a computer system,

with fraudulent or dishonest intent of procuring, without right, an economic benefit for oneself or for another.

It is important to understand that cybercrime is not limited to the destruction of computer systems and fraudulent conduct, as you can see from the types of cybercrimes listed in the Convention. The elimination of harmful content such as child pornography and the prevention of infringement of copyrights on networks are also extremely important issues. Conduct such as obstructing or interfering with electronic commerce on network systems also falls within the scope of cybercrime.

It is noteworthy that cybercrime is rather common on Japan. According to statistics released by the Japanese National Police Agency, the number of people arrested for cybercrimes has increased as indicated in the diagram.

	2001	2002	2003
Auction on the computer network	2,099	3,978	5,999
Fraud and related malicious trading	1,963	3,193	20,738
Defamation	2,267	2,566	2,619
Malicious contents	3,282	2,261	4,225
Unsolicited e-mail message	2,647	2,130	2,329
Unauthorized access, computer virus etc.	1,335	1,246	1,147
Others	3,684	3,955	4,697
Total	17,277	19,329	41,754

Table1: the number of complaints relating to Cybercrime

Also Table 2 shows an increase in the total number of arrested people in the past three years.

	2001	2002	2003
Unauthorized computer access	35	51	58
Computer crimes on Penal Code	63	30	55
(Illegal electromagnetic record)	(11)	(8)	(12)
(computer interference)	(4)	(4)	(9)
(computer Fraud)	(48)	(18)	(34)
Other crimes by means of network systems	712	958	1,083
(prostitution of children)2	(117)	(268)	(269)
(child pornography)	(128)	(140)	(102)
(fraud)	(103)	(112)	(86)
(obscenities)3	(103)	(109)	(113)
(Intimidation)	(40)	(33)	(38)
(copyright infringement)	(28)	(31)	(41)
(defamation)	(42)	(27)	(46)
Total	810	1,039	1,196

Table 2: the number of arrested persons relating to computer crimes

In response to these developments in cybercrime, the Japanese government is

[2] The prostitution of children has been taking place mainly at the meeting points on the Web or via mobile phones.
[3] This number doesn't include the number of child pornography.

revising laws such as the Criminal Code and the Code of Criminal Procedure. Of course, like China, Japan has a law penalizing unauthorized access to information systems. Many cybercrimes, however, are not limited to just unauthorized access. Consequently, among the proposed revisions to Japanese law is one to penalize the production of unlawful computer software such as computer viruses.

Proposed amendment bill of the Penal Code

Art. 168bis

1. A person who has, for the purpose of use for computer systems of another person, produced or provided an electromagnetic record or other records as follows shall be punished with penal servitude for not more than three years or a fine not more than five hundred thousand yen;

(1) an electromagnetic record which gives a wrongful instruction to the electronic computer systems of another person by making them not to act to be fit for the purpose of proper use or making them to act contrary to the purpose of proper use;

(2) in addition to those provided for in the preceding subparagraph, an electromagnetic record or other records in which the wrongful instruction under said subparagraph has been recorded.

2. The same shall also apply to a person who has used the electromagnetic record under paragraph 1 for computer systems of another person.

3. Attempts of paragraph 2 shall be punished.

Art 168ter

A person who has, for the purpose of paragraph 1 of the preceding Article, obtained or retained the electromagnetic record or other records under subparagraphs of the said paragraph shall be punished with penal servitude for not more than two years or a fine not more than three hundred thousand yen.

5 Computer Securities

Even if we respond to cybercrime by penalizing it, there are issues that cannot be addressed until after a cybercrime has been committed. As a result, efforts to prevent cybercrime, and when cybercrime does occur, to take technological measures to minimize the harm resulting from cybercrime are also needed. This type of technology measure is referred to as computer security.

There is even a field of scholarship that researches methods for preserving electronic and other evidence that establishes that a cybercrime was committed, analyzes it, and presents it to courts. This field of study is generally referred to as computer forensics.

Computer security is an extremely important issue in all countries. Moreover, there are numerous issues that require global efforts to enhance computer security.

In 2002, the Organization for Economic Cooperation and Development issued a document entitled OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security4. Countries around the world are observing these guidelines and adopting them as their national security policies.

Aims:

These Guidelines aim to:
− Promote a culture of security among all participants as a means of protecting information systems and networks.
− Raise awareness about the risk to information systems and networks; the policies, practices, measures and procedures available to address those risks; and the need for their adoption and implementation.
9
− Foster greater confidence among all participants in information systems and networks and the way in which they are provided and used.
− Create a general frame of reference that will help participants understand security issues and respect ethical values in the development and implementation of coherent policies, practices, measures and procedures for the security of information systems and networks.
− Promote co-operation and information sharing, as appropriate, among all participants in the development and implementation of security policies, practices, measures and procedures.
− Promote the consideration of security as an important objective among all participants involved in the development or implementation of standards.

Principles:

1) Awareness
Participants should be aware of the need for security of information systems and networks and what they can do to enhance security.

2) Responsibility
All participants are responsible for the security of information systems and networks.

3) Response
Participants should act in a timely and co-operative manner to prevent, detect and

[4] http://www.oecd.org/dataoecd/16/22/15582260.pdf

respond to security incidents.

4) Ethics
Participants should respect the legitimate interests of others.

5) Democracy
The security of information systems and networks should be compatible with essential values of a democratic society.

6) Risk assessment
Participants should conduct risk assessments.

7) Security design and implementation
Participants should incorporate security as an essential element of information systems and networks.

8) Security management
Participants should adopt a comprehensive approach to security management.

9) Reassessment
Participants should review and reassess the security of information systems and networks, and make appropriate modifications to security policies, practices, measures and procedures.

Proper implementation of computer security and computer legal science requires the training and of large numbers of computer engineers and security professionals. Even as technologies to protect against cybercrime are developed, cyber criminals are developing ever more ingenious criminal methods. This is apparent from examples such as computer viruses and hacking. In response to new criminal methods, even more effective technological means must be developed as quickly as possible. The security of electronic commerce also requires the development of more powerful encryption systems and electronic certification technologies.

It is even more important, however, that these technological responses be developed and implemented with suitable legal scholars. As a result, demand for legal scholars who specialize in cyber law will increase dramatically. I imagine that the demands and necessity on cyber law in both China and Japan are as yet not fully understood.

6 Conclusions

I have discussed cyber law, primarily from the perspective of cybercrime. Of course, cyber law deals with many issues other than cybercrime. Electronic commerce and the

protection of intellectual property rights to electronic content are just two on the major aspects of cyber law.

China is undergoing dramatic development, but I believe that there is a strong awareness concerning the importance of cyber law. In the future, the study of cyber law will take place on a global scale, and it is my sincere wish that people around the world will be able to engage in electronic economic activities safely.

Thank you.