Comparative Research on "Convention on Cybercrime" and Chinese Relevant Legislation

Pi Yong*

Since 80's last century, Cybercrime has caused serious damage to Chinese society. In order to control Cybercrime, China started to make relevant legislations on Cybercrime. Until now, the relevant legislations on Cybercrime in China can be classified into two parts, the substantive law and procedure law. This paper below will make a comparative research on "Convention on Cybercrime" and Chinese relevant legislations.

Chapter I The Comparison of Chinese Cybercrime Substantive Law Legislations with Relevant Provisions in "Convention on Cybercrime"

The relevant Chinese criminal laws which are specific to Cybercrime are Articles 285, 286 and 287 of "Criminal Law of the People's Republic of China", as well as the "Decision of the Standing Committee of the National People's Congress on Ensuring the Internet Security". The crime of infringing on the security of computer information system in Article 285, 286 of "Criminal Law of the People's Republic of China" include the crime of illegally invading computer information system and the crime of destroying or damaging computer information system. The offenders, who use internet to commit the crime mentioned above, shall be convicted and punished in accordance with the above two offences. Article 287 of "Criminal Law of the People's Republic of China" and the "Decision of the Standing Committee of the National People's Congress on Ensuring the Internet Security" indicate that by using computer or internet anyone, whose conduct brings serious damage to the society and is convicted a crime rather than which mentioned above, shall be criminally responsible in accordance with the relevant criminal laws. So Article 287 and the Decision together with other relevant criminal provisions are about other computer and internet related network crime.

1. Infringing the Security of Computer Information System

(i) Illegal Invasion of Computer Information System offence

Article 285 of Chinese Criminal Law states that, in violation of State regulations, invasion into the computer system of State affairs, national defence establishment, or sophisticated science and technology, constitutes the criminal offence of illegal invasion into a computer system. This crime is similar to the crime model of illegal access to a computer system in the "Convention on Cybercrime", and both of them are focused on the unauthorized conduct of intentionally accessing a computer system. The main difference is that the criminal object of the crime in Article 285 lies in computer information system in the fields of State affairs, national defence establishment, or sophisticated science and technology. Moreover the object shall not be limited to a single

* Pi Yong, Professor of School of Law of Wuhan University, P.R.C.

computer system, and it shall include other relevant network equipment related to the computer system.[1] If the offender invades into the computer network of the three areas specified above but did not invade into their computer system, he may be convicted of the offence of illegal invasion into a computer information system. Article 285 therefore focuses more on the protection of a specific computer system and the integrity of the system within the related area. In contrast, the object of the crime model in the Convention is not limited to these three fields. Illegal access to any computer system (including State, corporate or personal computer system) is considered a criminal offence In other words, the crime model in the Convention focuses more on the security protection of various computer systems.

In view of protecting the development of the information society, the author believes that the target of protection in Article 285 is too . Many computer systems in those important fields, such as air transportation, public transportation and hospital, cannot be protected under the Chinese Criminal Law. In contrast, the crime model of the Convention reflects the focus of criminal law with the basic unit of information society.

(ii) Damage of Computer Information System Offence

Article 286 of Chinese Criminal Law defines the crime of destroying or damaging computer information system as follows: (1) in violation of State regulations, deletes, alters, adds or interferes the functions of the computer information system,, rendering failure of the computer information system to operate as normal and consequences are serious; (2) in violation of State regulations, deletes, alters or adds the data stored in, or handled, or transmitted by the computer information system or its application program and the consequences are serious; (3) intentionally creates, circulates destructive programs such as computer viruses, thus affecting the normal operation of the computer information system and the consequences are serious.

The first and third criminal conducts in Article 286 of Chinese Criminal Law are similar to Article 5 of the Convention, which defines the intentionally unauthorized conduct to obstruct the normal operation of the computer system and causing serious consequences. The difference between the two is that: the target of the former crime includes not only the computer data and application programs, but also the hardware equipment in the computer information system. For example, damaging the computer motherboard by using electromagnetic bomb; the object of the latter crime is the computer data (including the computer data and application programs in Chinese Criminal Law). The difference is that the latter conduct is committed through the network, therefore it is impossible to physically damage the hardware equipment of the computer system. If the former conduct is applied against the network only, then it would be basically consistent with the latter one.

The second criminal conduct in Article 286 of Chinese Criminal Law is similar to Article 4 of the Convention, which defines the criminal conduct of data interference. Both of these two articles focus on the intentional unauthorized conduct to infringe on the integrity and normal operation of

[1] Article 2 of the Provisions on Protecting the Security of Computer Information System of PRC says that computer information system means system including computer as well as other relevant equipment (including network equipment) which can collect, process, store, transmit and search data in accordance with certain rules.

the computer data as well as the application programs, which causes serious consequences. The main difference is: the target of the former criminal conduct relates to the data and application programs stored, processed or transmitted within computer system. The computer data and application programs stored outside the computer system are not the objects of the former one, which means that the conduct to delete, alter or add the data and application programs stored outside the computer information system, even if the consequences are serious, this conduct cannot be punished in accordance with the former article. The of the Convention relates to any computer data (including the computer data and application programs in Chinese Criminal Law), which is not limited to computer data stored, processed or transmitted within the system. The former article (Chinese Criminal Law), therefore, protects the data and application programs in the system in order to ensure the normal operation of the system, and the latter (Convention) article protects the integrity and normal application of the data The emphasis on is different between the two: under the Chinese Criminal Law, the destruction, or damage, of data within a system only is considered a crime, while under the Convention, the conduct alone is sufficient to constitute crime. In the author's view, ensuring the normal operation of a computer information system is just as important as preserving the integrity and proper use of the data itself in the regulation of the information community. Accordingly, the illegal interference of data as a criminal offence, in order to better protect activities relating to computer-related information.

Article 3 of the Convention defines the crime of illegal interception as "criminal offences 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" in order to protect the confidentiality of the transmission of digital data. In the Chinese Criminal Law, Article 252 states that, "concealment, destruction, or unlawfully opening another person's letter thereby infringing upon a citizen's right to freedom of correspondence, if nature is", the conduct constitutes to the infringement of freedom of correspondence offence. To a small degree, the crime of infringing the freedom of correspondence is similar to the crime of illegal interception, because both articles have the function of protecting the freedom of correspondence. However, the difference between the two is also very obvious: (1) the criminal object in Article 252 is the letters of citizens and this article protects the confidentiality and freedom of correspondence. Although the definition of letter could be extended to cover both a posted letter as well as an email, this definition could not cover all transmissions of digital data, such as during internet browsing or document upload. Article 3 of the Convention protects various non-public transmissions of computer data so that the scope is much larger, including human-human transmission of computer data, human-computer transmission of computer data, and even includes the illegal interception of electromagnetic radiation from the computer equipment. (2) The criminal conduct in Article 252 is concealing, destroying or unlawfully opening another person's letter. In Article 3 of the Convention the criminal conduct is intercepting transmission of computer data by technical means. There are various types of interceptions, such as invading into the computer system to obtain the data directly, or obtaining the computer data by using electronic interception equipment in the computer network and so on. In my opinion, in the information society, the main communication method is not by means of the traditional p, but by computer data transmission through the network. If the Chinese Criminal Law cannot protect the computer data transmission, it will

definitely facilitate the violation of computer data transmission, and it will be detrimental to the protection of the freedom and confidentiality of correspondence of citizens.

Article 6 of the Convention defines the crime of misuse of the devices as intentional unauthorized production, sale, procurement for use, import, distribution or otherwise making available or possession of the computer equipment or data which is used for the committing Cybercrime. In contrast, there is no similar provision in Chinese Criminal Law. If the offender produces, sells or procures such equipment or data in order to commit, or help others to commit, Cybercrime, he may not be convicted of a crime, or he may be punished under the offence of aiding or abetting. In the author's view, the computer equipment and data used for committing Cybercrime are very powerful and important criminal equipment. It not only helps the successful completion of the crime and avoids legal sanctions, but also strengthens and consolidates the criminal intent of the offender. The misuse of devices is therefore very important to the development of Cybercrime. In order to combat Cybercrime more effectively, we must control such dangerous conduct at the very beginning, conditions for committing a subsequent Cybercrime will be eradicated. The Chinese Criminal Law does have such provisions r control crime at its source. For example, Article 295 of the Chinese Criminal Law defines the crime of abetting. However, this crime is limited to teaching the method of committing a crime, and does not include the misuse of computer devices. It is recommended that, the Chinese Criminal Law establishes as criminal offences, the ,intentionally and without right, making available the computer password, access code, or similar data.

2. Other Cybercrime Related to Internet

The Chinese criminal legislation on other Cybercrime related to internet includes Article 287 of the Criminal Law, "Decision of the Standing Committee of the National People's Congress on Ensuring the Internet Security" and other relevant provisions in the Criminal Law. These provisions did not indicate under which offence these types of Cybercrime could be convicted. By analyzing the Cybercrime itself, however, under the Chinese Criminal Law, aside from certain crime which could not be committed physically through computer network devices (such as extort a confession by torture), or a crime which requires specifically defined method of commission, the majority of offences can be committed through computer network devices. Furthermore, due to the development of the information society, some crime, which could not be committed through internet before, can be now committed by using internet, for instance using internet to interfere with the telemedicine operation in order to commit murder. In fact, the majority of the crime in Chinese Criminal Law require no specific type for the commission method and criminal object (for example, the official document and certificate are not limited to tangible form), thus, regarding computer crime of forgery, fraud, infringing copyright and related rights as well as child pornography in the Convention, Chinese Criminal Law does have relevant provisions to rule. However, to some extent, these relevant provisions in Chinese Criminal Law are different from the respective provisions in the Convention. The differences will be discussed in the following paragraphs.

Article 7 of the Convention defines computer-related forgery, which establishes the criminal conducts as, 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. In the Chinese Criminal Law, there is no crime of forgery. In contrast, Chinese Criminal Law has defined various crime of forgery, such as the crime of forging stock, and the crime of forging State official documents etc. Since there is no specific form of criminal object required in these provisions, thus by using internet devices, committing forgery crime indicated in Chinese Criminal Law could apply to the relevant provisions directly, and there are no legal obstacle for the application. Article 8 of the Convention defines the crime of computer-related fraud. Chinese Criminal Law could be applied to the commission of various types of fraud through the use of internet.

Article 9 of the Convention defines the offences related to child pornography. The relevant provisions in Chinese Criminal Law are regulated in paragraph 1 of Article 363, paragraph 1 of Article 364, Article 366 and Article 367. The above provisions define the crime of producing, duplicating, publishing, selling or disseminating pornographic materials for the purpose of profit, and the crime of disseminating pornographic materials. Since the two types of crime above do not define any specific criminal method, the above provisions can be applied when they are through the use of internet or computer. However, the offences related to child pornography of the Convention do have differences with the two crime in Chinese Criminal Law: (1) the criminal object of the former (Convention) is the child pornography materials, so that the legislative purposes is to protect children against being used in sexual activities; the criminal object of the latter (Chinese Criminal Law) is the pornography materials including adult pornography materials as well as child pornography materials, so that the legislative purpose is to protect a good social environment. (2) the former criminal conduct is producing, offering or making available, distributing or transmitting, procuring or possessing child pornography through a computer system; the latter criminal conduct is producing, duplicating, publishing, selling or disseminating pornographic materials. (3) compared with the former one, paragraph 1 of Article 363 requires the purpose of making profit to convict the crime, so that the condition to establish this crime is stricter; the provision in the Convention only requires the purpose of distributing child pornography materials through computer system to convict crime. Paragraph 1 of Article 364 requires that the circumstances of disseminating pornography materials are serious in order to convict the crime; the provision in the Convention says that the offender shall be punished if he offers, distributes or transmits child pornography materials. From the comparison above, the conclusion is that combating child pornography crime and protecting children against being used in sexual activities have become a criminal policy recognized widely in the international society. In contrast, China lacks legislation against child pornography crime: The Chinese Criminal Law does not differentiate between child pornography crime and other crime of producing, selling and disseminating pornography materials. The crime of producing, selling and disseminating pornography materials have some shortcoming in dealing with child pornography crime. The present author suggests that special provisions should be established in the Chinese Criminal Law to combat child pornography crime, which infringes upon the basic right of children. Such provisions will promote positive, ,moral values in the society. special provisions for child pornography should include wider conditions for conviction, and establish more serious punishment. The Chinese provisions should also differentiate the crime related to adult pornography materials. The Chinese Criminal Law may consider adopting Article 9 of the

Convention to respond to the international call for legislation against child pornography crime.

Article 10 of the Convention defines the crime of infringing copyright and related rights. The corresponding provisions in Chinese Criminal Law are Article 217 and Article 218 which define the crime of infringing copyright and the crime of selling work reproduced by infringing copyright. Since in Article 217 and Article 218, there is no specific requirement for the criminal method, thus by using internet or computer devices committing these two crime can apply these two articles directly. However the difference between the crime of infringing copyright and related rights in the Convention, and the crime mentioned in Article 217 and Article 218 of Chinese Criminal Law is: the former provision from the Convention establishes the criminal offences of infringing copyright and related rights when such acts are committed on a commercial scale; the latter provisions in the Chinese Criminal Law requires not only the minimum standard of illegal income or serious circumstances, but also the purpose of making profit. In legal practice, the provisions in the Chinese Criminal Law may encourage copyright infringement which is committed through internet and computer devices, because the cost of mass reproducing or distributing other's copyrighted work is low, and if the perpetrator has no intention of making a profit, he cannot be prosecuted for criminal liability, even if his reproduction or distribution has brought an extremely heavy economic loss to the victim. The present author recommends that, when the Chinese Criminal Law is amended, "for the purpose of making profit" in Article 217 should be deleted. Instead, in these provisions, the infringement shall reach a certain scale, for example, the market value of the infringement shall reach a certain amount.

3. The Legislation on the Criminal Patterns of Cybercrime

Article 11 of the Convention states that, intentionally aiding and abetting others to commit the 9 types of criminal offences mentioned in the Convention shall bear criminal liability. In Chinese Criminal Law, the person aiding others to commit a crime is treated as an accomplice, and both the accomplice and instigator shall be prosecuted for criminal liabilities. Thus, regarding to the 9 types of Cybercrime in the Convention, except for those crime which are not defined in Chinese Criminal Law, such as the crime of illegal interception, misuse of devices and child pornography, the accomplice and instigator of the rest crime shall bear criminal liability.

According to the Chinese Criminal Law, an offender who attempts to commit a crime shall bear criminal liability. Thus, in principle, all offenders who attempt to commit the 9 types of crime defined in the Convention shall be prosecuted for criminal liability. However, the following criminal attempts are not prosecuted in the Convention: illegal access to the computer system, misuse of devices, infringing copyright and related rights, as well as the subsections (b), (d), (e) of crime related to child pornography.

4. Cybercrime Committed by a Unit

Article 12 of the Convention defines the corporate liability for committing as well as aiding, abetting and attempt to commit the 9 types of Cybercrime in the Convention. In the Chinese Criminal Law, only a part of the crime related to the 9 types of Cybercrime shall attribute criminal

liability to , for instance, the offence of infringing copyright.

Chapter II The Comparison of Chinese Cybercrime Procedure Law Legislation with Relevant Provisions in "Convention on Cybercrime"

With the development of computer and network technology, have increased rapidly. The use of electronic evidence in criminal investigation has posed new challenges to criminal legislation and practice. Since the offender of Cybercrime uses computer and network to commit crime, digital data stored in computer system or transmitted in internet has constituted very important evidence. In some circumstance, the digital data will become the key, or the only, evidence for convicting the offender. How to effectively collect digital evidence data, therefore, has become the first step to combat Cybercrime. After the amendment of the Criminal Procedure Law of the People's Republic of China in 1996, parts of the legal system which relate to in forensic investigation has become more comprehensive. Firstly, the Chinese Criminal Procedure Law defined the statutory authority to collect evidence in criminal cases. The statutory authority is the People's Court, the People's Procuratorate and the public security organs. State security organs shall, in accordance with law, handle cases of crime that endanger State security, performing the same functions and powers as the public security organs; the security departments of the Army shall exercise the power of investigation with respect to criminal offences that have occurred in the Army; crime committed by criminals in prison shall be investigated by the prison. Secondly, the Chinese Criminal Procedure Law defines the responsibility of units and individuals who are related to the criminal cases to assist the investigation. "Judges, procurators and investigators must guarantee that all citizens who are involved in a case, or who have information about the circumstances of a case, to objectively, and fully, provide evidence and, except in special circumstances, they may be brought in to assist in the investigation". When the People's Court, the People's Procuratorate and the Public Security organs collect, or obtain, evidence from the units and individuals concerned, "the units and individuals concerned shall provide authentic evidence". Thirdly, the Chinese Criminal Procedure Law has specifically defined the search and seizure of evidence in Section 5 and 6 of Chapter II, Part two, which contains 10 articles. Fourthly, Chinese Criminal Procedure Law has defined the system to invite experts to assist in the investigation, "when necessary, experts may be assigned, or invited, to conduct an inquest, or examination, under the direction of the investigators". All the provisions above, together with relevant judicial interpretations and administrative regulations, have formed the legal system of evidence investigation, as well as the legal basis for digital evidence investigation in criminal investigation in China.

Until now, in addition to the Chinese Criminal Procedure Law, the relevant laws or regulations, judicial interpretations and government departmental regulations contain: "Regulation on Internet Information Service of the People's Republic of China" and "Working Rules on Interim Regulation of International Networking of Computer Information Network" by the State Council, "Regulations on Internet Surfer Service Sites" by the Ministry of Information Industry, Ministry of Public Security, Ministry of Culture together with the State Administration for Industry and Commerce, "Provisions for the Administration of Internet Electronic Bulletin" by the Ministry of Information Industry, "Interim Working Rules on Internet Banking Service" by the People's Bank

of China, “the Notice from the Ministry of Education about the Provisions for the Administration of Internet Electronic Bulletin in Colleges and Universities” by the Ministry of Education, “People's Procuratorate Rules of Criminal Procedure” by the Supreme People's Procuratorate and “Procedural Rules for Criminal Cases by Public Security Organs” by the Ministry of Public Security. All the laws or regulations, judicial interpretations and government departmental regulations above stipulate various investigative measures for digital evidence.

1. Mandatory Requirement for the Internet Service Provider to Record and Preserve Relevant Information

This kind of investigative measure includes the following laws and regulations:

Article 14 of the “Regulation on Internet Information Service of the People’s Republic of China”: Internet information service providers, which provide news and publishing services as well as services such as electronic bulletin, shall record and provide the content of the information published, the time of publishing, the internet address or domain name of publishing; the internet access service providers shall record the information of the users such as their online time, their user names, internet address or domain names, telephone numbers called, and other information. Both Internet information service providers and internet access service providers shall keep the records for 60 days, and provide the records to relevant State authority when it is inquired.

Article 19 of the “Working Rules on Interim Regulation of International Networking of Computer Information Network”: The units which provide access port service to international network as well as the units which connect and access international network shall keep all the relevant information and documents related to the service they provide; shall in time provide relevant information and documents during inspections by the Information Work Leading Office of the State Council and other competent authorities. The units which provide access service to international network and connect to international network shall submit the reports about the network operation, business development, and administrative work of the previous year to the Information Work Leading Office of the State Council in February every year.

Article 10 of the “Regulations on Internet Surfer Service Sites”: The operator of internet surfer service sites shall fulfill the following duties:
…
(3) record the internet surfer information, keep the record for 60days and provide this information when inquired by competent authority in accordance with the laws…

Article 14 of the “Provisions for the Administration of Internet Electronic Bulletin”: The electronic bulletin service provider shall record the information content published in the electronic bulletin service system as well as the time of publishing, the internet address or domain names of publishing. The record shall be kept for 60 days and provide to relevant State authority when inquired in accordance with the laws.

Article 15 of the “Provisions for the Administration of Internet Electronic Bulletin”: The internet

access service provider shall record the information of the users, such as the online time, user names, internet address or domain names, calling telephone number and other information. The record shall be kept for 60 days and provided to relevant State authority when inquired in accordance with the laws.

According to the provisions above, we can summarize that the mandatory requirement for the internet service provider to record and preserve relevant information, as an investigative measure, has the following characteristics:

(1) the provisions above, which regulate internet service providers, are administrative laws and regulations. The purpose of these provisions is to require internet service providers to provide and preserve relevant information record, in order to assist the administrative law enforcement or criminal investigation. Such assistance is vital to the success of criminal investigation.

(2) in this investigative measure, the legal obligation lies with the internet service providers that can be classified as the internet information service provider and the internet access service provider. The internet information service provider engages in journalism, publishing and electronic bulletin services. The internet access service provider includes not only the internet access service provider, but also units which provide access port service to international network, as well as units which connect and access international network and the operators of internet surfer service sites. The former and the latter service providers bear different legal obligations. The access service provider is required to record and preserve the information of the users, such as their online time, user names, internet address or domain names, calling telephone number etc. In contrast, the information service provider is required to record and preserve the content of the information published, the time of publishing, the internet address or domain name of publishing and other traffic data.

(3) This investigative measure stipulates the legal obligation as recording information, preserving backup record, and providing the recorded information to relevant State authority when required. The backup record shall be preserved for 60 days. However, some exceptions apply: the units which provide access port service to international network as well as the units which connect and access to international network shall keep all the relevant information and documents related to the service they provide; shall immediately provide relevant information and documents during inspections by the Information Work Leading Office of the State Council and other related authorities. The units mentioned above shall record a wide range of information. Since the period of time for the preservation is not specified, the preservation of such information shall be permanent.

This measure is similar to Articles 16 and 17 of the Convention which stipulate “expedited preservation of stored computer data” and “expedited preservation and partial disclosure of traffic data” respectively. They are all measures of preserving digital data which may be used as criminal evidence. Although they are not directly used for collecting and obtaining evidence, these measures form the basis for digital evidence investigation and the preparatory steps for the

investigation of Cybercrime.

This measure in Chinese laws has some common characteristics with Article 16 and 17 of the Convention: firstly, both the Chinese legislation and the Convention require the internet service providers to preserve relevant information under their management and control. In other words, both provisions indicate that the investigative authority is not the one who preserves relevant information directly, instead, the internet service provider is required to burden the legal obligation of preserving relevant information in computer or network system. Secondly, inclusion of content data and traffic data in the information preserved is required in both the provisions. The object protected by the data preservation provisions in the Convention is stored computer data, especially traffic data. The relevant measures in China classify the data preservation into two types: For the internet access service providers, they are required to preserve traffic data, and for the internet information service providers, they are required to preserve the traffic data as well as the content of the data. Thirdly, both the Chinese measures and the Convention have stipulated that the preservation of data shall reach a relatively long period of time. The Convention stipulates that the maximum period of time for preservation could reach 90 days. If parties of the Convention preserve relevant data according to their mutual assistance treaties, the period of time for preservation must be no less than 60 days. In China, generally speaking, the period of time for preservation shall be 60 days. For specific units, they are required to permanently preserve information and data related to their service.

However, the Chinese measures do have some differences with Article 16 and 17 of the Convention:

(1) Compared the Chinese measures, the provisions in the Convention have a broader scope of application and more effective protection of digital evidence. The Chinese measures are applied only to internet service provider, which includes internet information service provider engaged in news, publishing and electronic bulletin services and internet access service provider such as the units which provide access port service to international network, as well as the units which connect and access to international network, and operators of internet surfer service sites, and does not include individuals. In contrast, the scope of application of the relevant provisions in the Convention has extended to individuals. According to the judicial order, the preservation could be applied to digital evidence which is stored in a personal computer system or network device, further preventing the loss of digital evidence.

(2) The contents of requirements are different with the Chinese measures and the Convention. The Chinese measures require internet service provider to record, preserve the traffic data or the content data generated from their service. Thus, regardless of whether or not the data is related to the criminal case investigated, the service provider bears the legal obligation of preserving data mentioned above. Under the Convention, the provisions stipulate measures of “data protection” rather than “data preservation”. There are two methods for “data protection”: one method is to enable the competent authorities to order or similarly obtain the expeditious preservation of specified computer data; the other method is to order a person to preserve specified stored computer data in the person’s possession or control. The second

protection method is similar with the Chinese measures. However the Convention stipulates that the competent authorities can only order the service providers or individual persons to preserve the data that is related to specific criminal cases and already stored in their computer system, which means that the requirement in the Convention is not that high. The competent authorities cannot ask the service provider to record, preserve data or make technical update just for the purpose of preserving all information and data. Moreover, the data preserved is not limited to traffic data and content data. Other digital evidence related to the criminal case could still be the object of preservation, for example the electronic "trace" after invading into a computer system. In conclusion, the preservation in the Convention is really a protection of digital evidence. Compared to data preservation in the Convention, the method of digital evidence protection in Chinese measures is of a single mode, and the scope of digital evidence protected is too narrow. However, the Chinese measures do bring a heavy burden to internet service providers.

(3) The period of time for the data preservation is different. The Chinese measures ask for a 60 days preservation of the relevant data; for special units, the preservation shall be permanent. In the Convention, a judicial order for data preservation shall be no more than 90 days. If necessary, the relevant authority may issue a subsequent order for preservation, so that the period of time for preservation will be recalculated. In order to fulfill obligations of mutual assistance agreement, the party protecting data according to request shall protect the data for no less than 60 days. In the author's view, the period of time for preservation stipulated in the Chinese measures is too rigid that cannot reflect the real need of investigation. If the investigation organ discovers the digital evidence after the statutory period of time, they may lose this important evidence because they cannot order the internet service provider to continue preserving the relevant evidence. On the other hand, the obligation of permanent data preservation for some special units undoubtedly makes their burden heavier and this kind of obligation is difficult to follow in practice. By contrast, the provisions in the Convention are more flexible and for data preservation, they stipulate different period of time according to different requirements of investigation.

(4) In the balance between combating crime and protecting human rights, the Chinese measures are different with the Convention. Personal data is closely related to personal privacy. In the data protection or preservation with the purpose of investing criminal evidence, personal privacy will be inevitably violated or threatened. Hence, the two should be balanced while developing stringent data preservation measures. This reflects the pros and cons in the development of data preservation legislation. The Chinese measures consider less about the protection of human rights,[2] and have no restrictions for internet service providers on recording and preserving personal data.[3] Moreover, the provisions of preserving relevant data in the Chinese laws might become a lawful excuse for those internet service providers to collect and obtain personal information of the users. But in the Convention, it stipulates that

[2] Only in Article 12 of the "Provisions for the Administration of Internet Electronic Bulletin": electronic bulletin service provider shall keep the information of the users confidential, without agree of the user concerned, they shall not disclose the information, except as otherwise stipulated by law.

[3] Through collecting and analyzing personal data, personal living habits can be found, such as shopping preferences, habits or characteristic, etc. This analysis, as an important reference for developing clients, may disturb the normal life of the person concerned.

the data preservation measures shall follow Article 14 and 15 of the Convention, comply with the statutory obligation of protecting human rights and guarantee the principle of proportionality. The relevant measures stipulated in the Convention are more effective in protecting human rights.

(5) The degree of comprehensiveness in data preservation is different between the Chinese measures and those taken by the Convention. Computer data preservation is the premise for collecting and obtaining evidence. If data preservation cannot be kept confidential, the criminal suspects may destroy the protected data, thus affecting subsequent investigation. Confidentiality should be one of the vital components of data preservation measures. In this aspect, the stipulation in the Convention is more comprehensive, because it requires the custodian or other person who is to preserve the computer data to keep confidential the undertaking of such procedures, when asked to provide assistance to competent authority in accordance with law. In contrast, the Chinese provisions do not directly stipulate the confidentiality requirement. In practice, the units which preserve the relevant data are seldom required to keep the undertaking of such procedures confidential.[4]

In summary, although the Chinese mandatory stipulations, which require the internet service provider to record and preserve relevant data, can facilitate computer forensic investigations, the scope for digital evidence protection is still too narrow. Furthermore, the stipulations have brought heavy burden to internet service provider; the period of time for data preservation lacks flexibility, the privacy rights of citizens as well as other rights are inadequately protected; the data preservation measures are not comprehensive, hence the need for further advancement.

2. Seizure of Digital Evidence

Digital evidence is a type of electronic information which is invisible and is dependent on storage medium.. The seizure of digital evidence can be divided into two types: one type is to seize the storage media with the original digital evidence by using traditional seizure measures; the other type is to prohibit others from accessing the original digital evidence, and at the same time the investigation organs will obtain the copies of the original evidence. In order to become a new seizure measure, the latter type must resolve two issues:: the first issue relates to the legal effect of obtaining the copies of digital evidence; the second issue relates to legal procedure applied by investigation organs to collect and obtain copies which have legal effect. Although there are some provisions about seizure of digital evidence in the Chinese laws, the provisions are not specific and without clarity. Until now, the relevant laws and judicial interpretations include:
Article 116 of the "Criminal Procedure Law": If the investigators deem it necessary to seize the mail or telegrams of a criminal suspect, they may, upon approval of a public security organ or a People's Procuratorate, notify the post and telecommunications offices to check and hand over the relevant mail and telegrams for seizure. When it becomes unnecessary to continue with a seizure, the post and telecommunications offices shall be immediately notified.

[4] Article 52 of the "Procedural Rules for Criminal Cases by Public Security Organs" stipulates that in order to obtain criminal evidence, the technical investigation measures shall be kept confidential. However, the data protection by internet service provider in accordance with laws is not within the scope of technical investigation measures.

Article 188 of the “People's Procuratorate Rules of Criminal Procedure”: the documented evidence and audio-visual materials obtained shall be original copies. If it is very difficult to obtain the original evidence or due to confidentiality requirement, a copy of the original evidence may be obtained instead.

The material evidence obtained shall be original. If the original one is not suitable for moving or maintaining, or in accordance with the laws it shall be returned to the victim, or for confidentiality requirement it cannot be obtained, a photograph or video of the original evidence may obtained. The photograph or video taken shall be sufficient to reflect the original form and contents.

Obtaining the copy or copies of the documentary evidence and audio-visual materials or obtaining the photograph or video of the material evidence shall attach the notes to explain the reason why the original one cannot be obtained, the process of obtaining this copy, or photograph, or video, and the place where the original one is stored. The signature or seal of the custodian of the original evidence and the personnel who produced the copy, or photograph, or video, shall be provided with the explanatory notes.

Article 192 of the “People's Procuratorate Rules of Criminal Procedure”: If the investigators deem it necessary to seize the mail, or telegrams, or email, of a criminal suspect, they may, upon approval of a Chief Prosecutor, notify the post and telecommunications offices, or the internet service unit to provide the relevant mail, telegrams or email for seizure. When it becomes unnecessary to continue a seizure, the post and telecommunications offices or the internet service unit shall be immediately notified.

The provisions above have the characteristics as follows:

(1) The provisions are targeted at those mail or telegrams under the control of the post office and telecommunication office or internet service agency (including email and EDI). Firstly, the application object of these provisions is mail and telegrams. Other digital data, such as computer document or computer program etc, is not within the scope. Secondly, the mail or telegrams seized must be already under the control of post office and telecommunication office or internet service agency, otherwise the organization is unable, or will encounter difficulties, to fulfill the statutory obligation of seizure. The “control” here shall be interpreted as in the computer system or network system which is under the possession of the post office and telecommunication office or internet service agency, and the targeted evidence can be obtained and controlled by using existing technology of the post office and telecommunication offices or internet service agency. Even though the mail or telegrams in the computer system of an individual person can be obtained by the post office and telecommunication office or internet service agency through the use of certain technical means, as in the case of hacking into a suspect’s computer system to obtain mail or telegram, such mail and telegram cannot be regarded as that which come under the control of the post office and telecommunication office or internet service agency..

(2) The content of the provisions is the order for the post and telecommunication offices or internet service agencies to control mail and telegrams of the suspect. So the mail and telegrams seized are specific, which can only be the mail and telegrams of the suspect. The mail and telegrams of others cannot be seized; moreover the data filtering for finding investigation clues is prohibited.

(3) The seizure in the provisions shall follow legal procedure to issue judicial order to the post and telecommunication offices or internet service agencies. The judicial order must be approved by a public security organ or a People's Procuratorate, and in this judicial order the suspect, whose mail or telegrams need to be seized, shall be specified. When it becomes unnecessary to continue a seizure, the post office and telecommunications office or the internet service agency shall be immediately notified to lift the seizure.

The seizure of digital evidence in Chinese stipulations has something in common with Article 19 of the Convention which stipulates the seizure of stored computer data, for example asking the assistance of relevant parties, the object of seizure is digital data etc. Meanwhile, they have very obvious differences as:

(1) The scope of seizure object is different. The seizure of digital evidence in Chinese stipulations is limited only to mail in electronic type, such as email and EDI; the provisions in the Convention contain all computer data, including email and computer data in other use. So the scope of seizure object in the Convention is wider.

(2) The content of stipulations is different. The Chinese stipulations require the post office and telecommunications office or the internet service agency rather than the investigation authorities themselves to seize the targeted mail. The Convention stipulates that the investigation authorities seize relevant digital data and it further stipulates 4 specific ways of seizure. In the author's view, if the digital evidence is seized by other units rather than the investigation authorities, the digital evidence might be easily modified, damaged or lost, rendering challenges for the effective preservation of integrity and authenticity of the evidence. During the seizure process by the post office and telecommunications office or the internet service agency, if the digital evidence is modified or deleted, this will cause a serious impact to the following-up criminal procedural activities. The seizure of digital evidence therefore, should be conducted by investigative authorities. Regarding technical difficulties which might be encountered by the investigation authorities, subsection 4 of Article 19 stipulates that competent authorities can order anyone who has knowledge about the functioning of the computer system or measures applied to protect the computer data therein to provide, as is reasonable, the necessary information, to enable the undertaking of the search and seizure measures. Therefore, the seizure measures in the Convention not only ensure integrity and authenticity of the seized digital evidence,, they also facilitate convenience for investigative authorities..

(3) The degree of comprehensiveness for the related measures is different between the Chinese stipulation and the Convention . Searching and finding criminal evidence is the premise of

seizure of evidence, otherwise the object of seizure cannot be identified. If the digital evidence (the object of seizure) and its location cannot be identified in advance, the seizure measure cannot be applied to the wide spectrum of information. It is therefore necessary for laws to stipulate special searching measures for digital evidence. The Chinese laws lack such special stipulations, while the Convention stipulated the searching measures for computer data in detail. . Furthermore, the Convention combines search and seizure as a whole, hence seizure measures of digital evidence could be effectively enforced.

(4) In the protection of human rights, the Chinese stipulation and the Convention are different. The former one has no content related to human rights protection; the latter one has stipulated a special paragraph for protecting human rights, for example, providing certain compensation to the witness or experts invited, or sending notice before the seizure, etc.

In summary, a relatively wide gap exists between the relevant Chinese stipulations of digital evidence seizure and the search and seizure measures in the Convention with respect to the scope for application, content of the stipulations and related measures, and the protection of human rights.

3. Real-time Collection and Production Order for Computer Data

In Chinese criminal procedure laws, there are no stipulations for the measure of real-time collection of computer data. But in "State Security Law of the People's Republic of China" and "People's Police Law of the People's Republic of China", they define one of the technological means of reconnaissance as secret interception.[5] If the "secret interception" is interpreted broadly, it does share similarities with the measure of real-time collection for computer data. For example, both the secret interception and real-time collection measures real-time monitor and record the communications of the person concerned, without notifying him or her in advance. However, the Chinese technical reconnaissance measures do have certain flaws and these measures cannot replace the real-time collection measure. The reason is: while there are technical reconnaissance measures in relevant Chinese stipulations, there are only internal stipulations of relevant authorities, but no legal and clear statutory stipulations for the content of these measures, scope of application, essential requirements of application, right of approval and the procedure for approval, how to use the result of the investigation, or relief procedure. . The technical reconnaissance measures, including secret interception, are mandatory measures which may seriously affect the rights of citizens. Relevant Chinese legislations should be made more comprehensive, and statutory provisions in judicial practice should be strictly enforced if such special investigation is to be appropriately and effectively applied, and if violation of citizens' basic rights is to be avoided. Currently, however, relevant Chinese legislations are inadequate, and approval procedure lacks clear statutory stipulations, posing challenges to the attainment of the above two goals. Therefore, in order to effectively combat new forms of crime with the

[5] Both the "State Security Law of the People's Republic of China" and "People's Police Law of the People's Republic of China" has stipulated that after going through strict approval procedures, State security organs and public security organs may employ technological means of reconnaissance. The academic society and judicial practice society in China all agree that the secret interception belongs to the technological means of reconnaissance.

application of information technology and effectively protecting the rights of citizens, it is necessary for China to establish real-time collection measure for computer data.

Chinese legislations do not have any provision relating to production order of computer data.