Anti-circumvention Rules in the Information Network Environment in the US, UK and China: A Comparative Study

Jia Wang
Stellenbosch University School of Law, West Cape, South Africa
jajaishere@yahoo.co.uk

Abstract: This paper examines the impact of the technological measures that copyright holders employ to lock their works and discusses why users are disadvantaged. It compares the anti-circumvention rules in the Digital Millenium Copyright Act in the US and the Copyright, Patents and Designs Act in the UK; the latest exemptions to circumventing activities released by the US Library of Congress are included. It reviews the evolution of Chinese anti-circumvention rules, starting with a well-known case preceding the promulgation of the anti-circumvention rules, then it examines the anti-circumvention provisions in the Copyright Act 1990, the Software Regulation 2001 and the ISP Interpretation 2004. It also critically analyzes the latest Network Regulation 2006 by comparing it with the DMCA and the CDPA. The paper suggests that the Chinese anti-circumvention rules need to be constructed with more legal certainties. Recommendations are also made for additional redrafting to make China's anti-circumvention rules more adaptive to a digital environment.

Keyword: intellectual property law, copyright, technological measures, anti-circumvention law, China

1. Introduction

Circumventing technology is not new. Circumventing technologies and devices have been employed to decrypt digital versatile discs (DVDs), [1] Software [2] and to circumvent many other digital products.[3] Circumvention is increasing rapidly, particularly in the information network environment.[4] Copyright holders reproach consumers and users for circumventing technological barriers meant to prevent unauthorized or unlawful use of copyrighted material.[5] At the same time, copyright holders are criticized for controlling access to their works which restricts the public's access to information, stifles fair use and excludes the application of copyright law.[6] Therefore, copyright law serves as a balance between copyright proprietors and the public as it demarcates the legitimate line for circumvention and anti-circumvention acts and devices. Technology can enforce copyright law, but it should not compete or replace the law.[7] It thus requires the deliberations of legislators to adjust and create innovative anti-circumvention rules that address digital technology and information network challenges.

Anti-circumvention rules are considered to be a substantial extension of copyright protection because they extend legal protection to the technological area of copyright protection.[8] Therefore, to understand and to establish pragmatic anti-circumvention rules is particularly important for a developing country such as China. One of China's legislative tasks is to incorporate anti-circumvention rules into its intellectual property law in order to have an effective copyright protection mechanism that deals fairly with actors in the information network.[9] Not only China, but other developing countries also need to confront and deal with this problem. China's legislative experience in this area can serve as a valuable example to other developing countries.

This paper analyzes the Chinese anti-circumvention rules with particular reference to the information network environment by comparing the Digital Millenium Copyright Act [10](hereafter referred to as DMCA), the European Copyright Directive [11](hereafter referred to as EUCD) and pertinent Chinese legislation. This is done in five sections. First, there is a brief examination of the nature of anti-circumvention rules in order to provide a theoretical foundation for the study. Here relevant digital technologies are explained. Second, four aspects of the relationship between the DMCA and the CDPA are compared as reference points for the analysis that follows on China's anti-circumvention rules. Third, there is a review of China's anti-circumvention rules in the current legislation, namely the Copyright Act 1990,[12] two Regulations and a judicial interpretation.[13] This is followed with a comparison of four aspects of the Regulations on the Protection of the Right of Communication via Information Network[14] (hereafter referred to as Network Regulation) with references to the DMCA and the CDPA. Fourth, a tentative recommendation is made for a possible further redrafting of the Chinese anti-circumvention rules. This is followed with a summarizing conclusion.

2. The Digital Technologies and Anti-circumvention Rules'

Technological measures for information protection are based on cryptography and other technical measures [15],which attempt to control or restrict access or reproduce digital media content with electronic devices.[16] Widely used digital rights management (DRM) contains such technological measures as digital encryptions, virtual containers and watermarks.[17]

Once the threshold of digital technology was crossed, the reproduction of copyright materials became instantaneous and almost costless. The information network, particularly the Internet, is a powerful means that facilitates the dissemination of information.[18] Circumventing technology is also disseminated, thus making copyright holders vulnerable to piracy and other copyright infringements.[19] Therefore, on the one hand, technological measures are believed to be advantageous in monitoring the reproduction of illegal copies and controlling rampant piracy.[20] On the other hand, technological measures are criticized for contributing to the privatization of information regardless of the statutory protection period[21] and undermining the copyright law in the sense that fair use cannot be fully recognized and enforced. Consequently there is a decrease in the dissemination of information.[22]

Anti-circumvention rules belong to the copyright law system. The copyright law's utilitarian goal of promoting knowledge is widely acknowledged as a principle by national laws and international treaties.[23] Anti-circumvention rules, functioning as a component of copyright law, also promote public learning and encourage innovation. Copyright law adapts to technology developments.[24] Over the most recent decade, anti-circumvention rules have become a controversial issue amongst scholars, copyright holders and the public.[25]

The anti-circumvention provision first appeared in the WIPO Treaties 1996[26] and was first implemented by the US in the DMCA 1998. In 2001, the European Union enacted the European Copyright Directive[27] that also contained anti-circumvention rules. The United Kingdom amended its Copyright, Designs and Patents Act[28]（hereafter referred to as CDPA）in 2003 to bring the EUCD into its domestic legislation.[29] In particular, section 296 was amended to contain the anti-circumvention provisions. China revised its Copyright Act in 2001 for accession to the World Trade Organization (WTO)[30] in which a general anti-circumvention rule is included. A supplementary provision of the Copyright Act states that regulations for the protection of computer software and the right to communicate information via a network is to be established separately by the State Council.[31] In 2002, the Regulations on the Protection of Software[32] (hereafter referred to as Software Regulation) came into force with a nearly identical rule.[33] The Network Regulation issued in 2006 implemented the anti-circumvention rule with concrete provisions.[34] Most recently, China ratified the WIPO Treaties on December 29, 2006. Further legislative reform on copyright law, including anti-circumvention rules, is imminent.

3. Comparison of the Anti-circumvention Rules in the United States and United Kingdom

The US has been a pioneer in bringing the anti-circumvention rules contained in the WIPO treaties into its domestic legislation. Due to pressure brought by the US, the EUCD was formed after the DMCA. Although their rules are somewhat similar, there are major differences between the US and the European Union approaches. The EU member states basically followed the EUCD approach, but different nations construed the anti-circumvention rules with different provisions.[35] Among these countries, the United Kingdom serves as an example of national implementation of anti-circumvention rules.

In the amended CDPA, copyrighted software is treated differently from other digital copyrighted works in order to follow the requirements of the Software Directive.[36] Additional provisions that relate to other digital copyrighted works are a new area for the digital copyright law.[37] These additional provisions are analyzed as follows.

3.1 The Definition of an "Effective Technological Measure"

In general, both the DMCA and the CDPA divide technological measures into two categories: 1) technological measures that control access to a work; and (2) technological measures that control the copy of a work.[38] The DMCA has defined an effective technological measure as one that effectively controls access to a work as being the application of information, or a process, or a treatment requiring the copyright owner's authority to gain access.[39] The CDPA stipulates an effective technological measure as one could control access and copy.[40]

In comparing the two provisions, a notable difference is that the DMCA grants absolute protection to the access-control technological measures and partial protection to copy-control technological measures, while the CDPA grants protection to both types of technological measures.[41] Common to both is that any material can be protected by technological measures, regardless of copyrightability.[42] Case law also illustrates this.[43]

3.2 The Circumstances under which Violation of Anti-circumventing Rules Lead to Liabilities

The two legislation contain circumventing-act prohibition and device prohibition. They both adopt the approach of assigning liabilities on the basis of violation of technological measures rather than on the basis of an infringement of a copyright. This differs from the liability norm set in the Berne convention.

Four major differences are observed. First, in the DMCA liabilities are triggered simply with the violation of technological measures,[44] while in the CDPA the liability trigger is "intention" and "knowledge".[45] Second, the DMCA has adopted a minimal approach with liability flowing from the violation of technological measures that control access, while the CDPA takes a comprehensive approach with liability flowing from the breach of both technological measures that control access and copy. Third, with the DMCA there are two types of violation: 1) there is a basic prohibition to prevent the circumvention of technological measures that control access and the trafficking of circumvention devices and the provision of services;[46] and, 2) there is an additional prohibition.[47] This one does not prohibit the circumventing act itself. Therefore a person can engage in a prohibited usage of a work that he has lawful access, but someone who aids him by publicly offering devices, service, etc. to achieve the technological breach is liable.[48] The reason for the exemption of liability of the circumvention to a copy-control measure is to preserve fair use.[49] Fourth, the CDPA regulates that not only such device trafficking as in the DMCA violates the anti-device provision, but so does the possession of the aforesaid equipment.[50] Nevertheless, possession is only culpable for commercial purpose. Possession for private and domestic use is exempt.[51]

There have been wide discussions about a newly crafted "access right" for copyright holders.[52] This can strengthen copyright holders' monopolistic power over the copyright works, particularly if there is an absence of knowledge requirement in drawing violation liability.[53] Not only does it broaden the scope of the materials under the protection of technological measures,[54] but this right may also allow a longer protection period than copyright law grants. This disadvantages both of users and consumers.[55]

In terms of the exemption of liability of circumventing a copy-control technological measure in the DMCA, although circumventing for fair use usage is ostensibly preserved, there is a dilemma for users. Since a circumventing device is broadly defined,[56] without circumventing tools, ordinary users can not discover the materials they can use for fair use and circumvent copying.[57] Very simply, the preservation of fair use is somewhat empty.

3.3 The Definition of a Circumventing Device

In the DMCA, a circumventing device is defined broadly.[58] There are three categories of circumventing devices: first, is a device designed or produced primarily for the purpose of circumventing; second, is a device that has only a limited commercial purpose other than to circumvent and third, is a device marketed for use in circumventing. The CDPA mirrors almost verbatim the three categories.[59]

To define a device that has limited commercial use other than to be used as a circumventing device is a disservice to users and manufacturers since the device can be multifunctional. However, under the DMCA prohibitive provision, even a legitimate use is not exempt from prohibition. The substantial non-infringing use standard established in the *Sony*[60] case is modified by the DMCA.[61] In short, the strict prohibition of a circumvention device in practice nullifies fair use.

3.4 Exceptions

In the DMCA, the prohibitions in section 1201 are subject to a number of carefully crafted exceptions. Section 1201 (c) includes a fair use clause stating that nothing in section 1201 affects the rights, remedies, limitations or defense of copyright infringement, including fair use. [62] Section 1201 (d) to (i) are exceptions.[63] Section 1201(e) is a general exception to the application of the entire section on circumvention for law enforcement, intelligence and other such governmental activities.

The broadest of these exceptions in section 1201[64] establishes an ongoing administrative rule-making procedure to evaluate the impact of prohibiting circumventing.[65] The latest adoption of the six exemptions, for all intents and purposes, took place on November 27, 2006.[66] They contain three renewed exemptions granted previously[67] and three new classes of exemptions.[68] They are narrow in scope and apply to specific industries. They do not only pertain to the Internet, but rather to a broad multimedia environment. They do not exempt trafficking actions. A notable new exemption is the exemption for sound recordings on CDs protected by access controls. This creates security problems such as the rootkit distributed by Sony BMG CDs in 2005.[69] A well-known Chinese case, *KV300L++*, is somewhat similar to this one.[70]

The exceptions in the CDPA, in contrast to the DMCA, are loosely constructed. Section 296ZA (1) provides the grounds for anti-circumvention rules and states that anyone with knowledge or reasonable grounds to

know is held liable for circumventing technological measures. Section 296ZA (2) provides an exception for research on cryptography. The exception to circumventing devices is section 296ZB (3), which provides an exception for law enforcement and intelligence agencies to manufacture and use devices and services designed for circumvention. Section 296ZE provides a remedy when technological measures prevent permitted activities.[71]

A common concern that surfaced is the lack of a general exception.[72] The exceptions have come about as a result of negotiation and compromise among interested parties, namely the entertainment industry, the software industry,[73] publisher lobbyist groups,[74] and consumers and libraries.[75] However, the US Congress overlooked the fact that industries were not the only ones employing technological measures, for there were also "trade secret owners, privacy-seeking individuals" and others with confidential information.[76] Therefore, there is little room for future technological development by others than the current concerned industries. Another problem is that the anti-circumvention rules are often restrictively interpreted.[77] Without a general exception, the existing legislation is unduly harsh for users and ISPs since criminal sanctions apply when a violation occurs.[78]

4. Anti-circumvention Rules Related to Information Network in China

China's law makers need to understand the country's needs when they apply the anti-circumvention rules that have been borrowed from WIPO Treaties.[79] Comparing anti-circumvention rules with its counterparts in the US and UK would help China's legislators to identify the gaps in the current legislation and to better understand how to construct anti-circumvention rules with operability. It would be worthwhile for China to critically examine the legislative experience from both sides of the Atlantic and choose what is worthwhile as references when constructing rules of the same nature. The caveat is that the current legislative literature is far from perfect.[80] Since the US and the European Union are China's major trade partners,[81] a general consensus on the legal protection of such digital products as CDs and software would help to ameliorate copyright trade disputes and conflicts.[82]

4.1 The Evolution of the Anti-circumvention Rules in China

The lack of anti-circumvention rules was a concern among copyright holders, users, scholars and policy makers.[83] An example is the *KV300L++* case in 1997. An anti-virus software manufacturer, Jiangmin New Tech Ltd. (hereafter referred to as Jiangmin Ltd.) embedded an anti-piracy device called "logic lock" into its online update program which could detect an unauthorized software copy that was upgraded online and subsequently locked the C drive of the computer in which the unlawful software was running. Users who downloaded a program called MK300V4 could decrypt the KV300L++ program and then ran it. Worried that the circumventing program could make the market of the original software shrunk, some distributors downloaded it to test whether it worked or not and found their hard discs could not run after a trial.[84] Jiangmin Ltd. argued that there was no destructive effect on a computer when the logic lock locked the C drive, for it was only a lock, not a "bomb".[85] The legality of the logic lock was contentious.[86] Finally an administrative penalty of 5000 Yuan[87] was imposed on the ground that Jiangmin Ltd. had willfully inserted harmful data into a program and imperiled information network security.[88]

Two key issues pertaining to anti-circumvention rules in this case are (1) how to define an "effective technological measure"; should it be an *ex ante* defensive mechanism or should it be a self-remedy after an infringement? (2) Should there be an exception for circumvention for a security test as well as an exception for circumvention for a security reason? Additionally, how does one decide upon the liability of a software manufacture imbedding viruses, spyware or malicious software? Besides these concrete legislative concerns, there are also such issues as how to construct an anti-circumvention law among several options: to create a special code containing anti-circumvention rules as is the case in the US; to incorporate the anti-circumvention rules into the copyright act such as is done in the UK, or issuing regulations pertaining to anti-circumvention rules under the general guidelines in the Copyright Act? China's lawmakers need to reflect on these issues.

China joined the WTO in 2001. In order to meet the minimal requirements set by the Trade Related Aspects of Intellectual Property (TRIPS)[89] China has been involved steadily in a process of copyright reform.[90] The government approved copyright law amendments that brought China more closely into line with TRIPS and the Berne Convention.[91]

The first legislative response is the Copyright Act Amendment in 2001. Article 47 (6) states that anyone who "willfully circumventing or destroying the technological measures taken by a right holder for protecting the copyright or copyright-related rights in his work, sound recording or video recording, without the permission of the copyright owner, or the owner of the copyright-related rights", shall be subject to civil, administrative and criminal liabilities with penalties determined by circumstances. The Software Regulation contains an almost identical provision. Both provisions only apply to circumventing acts, not devices. The simplistic anti-circumvention rules facilitate the import, traffic and manufacture of circumventing devices within China. It also harms the software industry since circumventing technologies and devices for piracy are not prohibited. Since the two provisions are both very general, judges still are unable to deal with cases similar to KV300L++.

In addition to the Copyright Act and the Software Regulation, a judicial interpretation by the Supreme Court for regulating ISPs' legal status was revised in 2004（hereafter referred to as ISP Interpretation）. It provides that "an internet service provider, who knowingly uploads, disseminates or provides methods, devices or materials, which are specially used for bypassing or impairing technological protective measures for copyrighted materials, should be held liable for civil penalties under article 47 (6) of the Copyright Act by the people's court". It is doubtful the simplistic rule in this provision prejudices the internet service providers' legitimate rights for there was no definition of a "circumventing device". Moreover, the circumstances that apply discourage internet dissemination of information and stifles innovation.

4.2 A Critical Examination of the Relevant Provisions in the Network Regulation

China did not have concrete anti-circumvention rules after the *KV300L++* case for nearly a decade until the Network Regulation was introduced . The Network Regulation is of importance in the sense that it brings the general principle of the protection of communication right via the network into concrete and operable rules. The promulgation of the regulation indicates that China chose to regulate the circumvention by crystallizing the rules in the form of administrative regulation rather than a code or an act which is superior to administrative regulation.

After the amendment of the Copyright Act 2001, judges still felt that how copyright holders could exercise their rights, the scope of the fair use and how users could use compulsory license to obtain access to certain works are still lack of concrete guidance. Numerous cases arose as the result of the legislative gap.[92] In the light of the Chinese judicial system, if there is no code or act that regulates an object, the administrative regulation issued by the State Council has the primary authority. To adjust the relationship amongst the copyright holders, the ISPs, and the users, the Network Regulation has been promulgated.

According to the Legislative Affairs Commission under the Standing Committee of the National People's Congress, because the copyright protection in the network environment is new to legislators, and different jurisdictions have different approaches toward the level of protection, it is admitted by the officials that there were some questions still unclear to them; therefore, the Network Regulation leaves some issues with very general provisions and does not refer to some other issues at all.[93]

Nevertheless, despite the omission of some issues, the Network Regulation is a comprehensive legislation to respond to the lack of the rules that regulate the communication right via network compared with the preceding legislation. According to the characteristics of the communication right via information network, the Network Regulation puts forward four protective measures: (1) protect the communication right via network generally by requiring the users to obtain permission from and pay to the right holders, except where otherwise provided for in laws and administrative regulations; (2) protect the technological measures that employed by the right holders to guard the works, including the prohibition of the circumventing acts, devices and service; (3) prohibit the remove or alteration of the electronic rights management information of works and prohibit the provision of such works if known or should reasonably know the electronic rights management has been removed or altered; and (4) establish the summary procedure of "notice and delete". Among other things, the second measure targets the circumventing acts and devices, the following analysis will focus on the relevant provisions.

The anti-circumvention rules have not been judicially tested yet. The following sections examine the rules and compare them with the DMCA and CDPA rules to ascertain their merits and deficiencies.

4.2.1 The Definition of an "Effective Technological Measure"

In the Network Regulation an effective technological measure is a technology, a device or a component that prevents the public from accessing copyright owners' works, performances, sound and video recordings with an information network that is unauthorized or unlawful.[94] An effective technological measure here is broadly defined. Firstly, the language does not explicitly distinguish between a technological measure that controls access and one that controls copy. However, from the wording of "browse" and "appreciate" in the interpretation clause,[95] it is implied that technological measures could control access and usage such as copying. Secondly, it resembles the structure of s. 1201 in the DMCA that contains a "basic prohibition" and an "additional prohibition".[96] It not only proscribes circumventing acts and trafficking circumventing devices, but also prevents those who have already obtained lawful access to a work from a subsequent reproduction of the work and provide it to the public.[97]

This provision also touches on the legitimacy of a technological measure. A technological measure only should be defensive by controlling access in advance. Returning to the *KV300L++* case, the logic lock employed by Jiangmin Ltd was not legitimate in this sense.

4.2.2 Circumstances under which Violation of Anti-circumventing Rules Lead to Liabilities

The Network Regulation includes intention as a liability trigger for circumventing activities and trafficking of circumventing devices.[98]Compared with its US counterpart, the *scienter* requirement makes this anti-

circumvention rule more friendly to users.[99] Nevertheless, with the "additional prohibition" prohibiting further dissemination of a work after lawful access, it is questionable whether the *scienter* requirement is still justifiable as a liability trigger when a third party is involved in providing circumventing devices or services. Both in theory and practice in China, a joint intention is not a requisite for contributory infringement.[100] Otherwise it would be very difficult to identify an indirect infringer who assists or facilitates an infringement, therefore the remedies are difficult to reinforce. The *scienter* requirement could impose a copyright owner an unduly heavy burden of proof to launch an action against an indirect infringer.[101]

4.2.3 The Definition of a Circumventing Device

In the Network Regulation, articles 4 and 19 prohibit devices or components that are primarily used for the purpose of circumventing or impairing technological measures. A circumventing device is broadly defined. The general wording "primarily used for the purpose of circumventing" resembles the wording in the DMCA's first category of circumventing devices and the CDPA's third category which is almost the same.

4.2.4 Exceptions

The last sentence in article 4 generally states that circumventions otherwise permitted by law and administrative regulation are exempt. However, since the exceptions in the Copyright Act do not refer to digital technologies and an information network, it is doubtful if the exceptions in an analog world can be wholly converted to a network environment.

An exhaustive list of four exceptions in article 12 contains (1) those for education and scientific research given that the works, performances, video and audio recordings being circumvented are only available from an information network; (2) those for literal works to blind people for non-commercial purpose given that the literal works are only available from an information network; (3) those for judicial and governmental activities and (4) those for security testing. The four exceptions are subject to a general principle that users granted exceptions for access circumvention shall neither provide others with technology, devices or components for circumventing, nor prejudice right holders' other legitimate rights.[102]

Similar to the DMCA and the CDPA, it is notable that there is no general exception. Compared with the DMCA, the exceptions in the Network Regulation are more restrictive. The first exception, the education and research one narrows the scope of the materials that can be circumvented by stating the precondition of circumvention is the materials' sole availability from an information network. Moreover, the wording "scientific research" is ambiguous for it is uncertain what act qualifies as scientific research. Since China's software industry is still in its infancy, it needs a liberal approach for such technologies as reverse engineering and to carry on research dealing with the interoperability of software. There is also a need for students and researchers to study and develop cryptographical technology.

The second exception in the Network Regulation relating to blind people specifies that the circumvented content can only be literal works, and adds a prerequisite about its sole availability from the information network. The protection of minors and personal privacy are not on the exception list.

5. Recommendations and Conclusions

China needs to continue to construct its own anti-circumvention rules having both legal certainties to make the law operable and flexibilities to accommodate innovation. Firstly, in defining a technological measure, a narrow approach is preferable. The technological measures that control access and control copy should be explicitly distinguished. Exceptions to the prohibition are prescribed in a subsequent section of an anti-circumvention regulation. Along with defining technological measures, circumventing devices also need to be further clarified. To categorize a device solely used for circumventing as a circumventing device is favorable to equipment and software producers and users.[103] The sole purpose test enhances "certainty and ease of application".[104] Users then can worry less about inadvertently committing an illegal act and software designers and producers can be satisfied that they are unfettered in developing innovative programs.

Secondly, content that is protected by technological measures can be specified to only fall within copyright protection. In doing so, works already in the public domain or information that is not copyrightable will be open to the public. To give producers an economic incentive to collect and convert analogous materials into digital form, producers can be granted a right to claim compensation or charge a reasonable rate. This can be done either with an individual agreement or through a collective administrative entity. However, in the latter case copyright law may not be the appropriate regulation vehicle since such related laws as contract law would be a better choice.

Thirdly, article 4 only states in general terms that copyright holders can employ technological measures to protect their communication rights through an information network. To better protect copyright owners' rights, the purpose of technological measures could be enlarged, not only for communication rights, but also for the

protection of other related copyrights. To balance the interests between copyright owners and users it would be sensible to add a general statement that copyright holders seeking technological protection of their works, performances, and radio and video recordings not infringe consumers' privacy that is protected by law. By incorporating this immunity principle; no specific provision is needed in a subsequent section. Moreover, the judiciary is given more discretion.

Fourthly, when dealing with exceptions several amendments might be considered. Preferably, a general exception is created prior to specific exceptions. This leaves space for future technological development. Consequently, the anti-circumvention rules will have the flexibility to maintain legal stability in the future without frequent modification.[105] The protection of minors can be incorporated into a general exception without having a separate exception as is the case in the DMCA. Some scholars also propose that an on-going rulemaking system can help to adjust exceptions in a timely manner.[106] However, a feasible approach in establishing this rule assessing and making procedure is not yet clear.

In examining specific exceptions, the first exception category[107] is particularly problematic. The term "scientific research" is unclear. It needs to be clarified as to whether reverse engineering and decryption fall within the scope of scientific research if it is for a non-commercial purpose.[108] The law needs to distinguish the circulation and flow within an academic community of circumventing knowledge, technologies and devices from similar types of communication with the public. If this were to be done, a paper presented at a conference explaining security flaws in an operational system could be exempted.[109]

Currently, the exception to the provision about certain materials for education and scientific research purposes is only qualified when the material is provided to "a few" education and research staff members. The descriptive term "a few" is imprecise. Specific number of people needs to be specified within a range depending on the different size of the educational and research institutions.

Last but certainly not least, the legal status of ISPs was unclear in dealing with the liability for ISPs who upload and provide software or service that can be used for circumvention.[110] Article 7 of the ISP Interpretation states that an ISP who knowingly circumvents or provides a device or service to circumvent is liable. Thus "knowledge" is the determining factor in establishing liabilities.[111] Since the Copyright Act 1990 does not make ISPs responsible for censoring before uploading, in practice it may be difficult for ISPs to determine whether software or certain contents can be used for circumvention or not.[112] By extending the liability norm stipulated by the Copyright Act, the ISP Interpretation unreasonably burdened ISPs with more obligations. Therefore, to release ISPs' from risk when providing such services and encourage the dissemination of information via the internet, copyright holders can be required to detect illegal circumventing devices or services and ask the ISP to remove or delete the content or disconnect the hyperlink. If the ISP fails to act in due time, then the copyright holder can launch a legal action. In other words, a similar "safe harbor" principle can be inserted to safeguard ISPs' interests.[113]

Additionally, the widespread computer viruses, spyware and malicious software are salient phenomena along with the prevalence of the Internet. The KV300L++ case also concerned the computer virus issue since a virus was imbedded to prevent a software operation after circumvention. However, the Chinese anti-circumvention rules fail to address this issue. The new exemption in DMCA for the circumvention of flaws imbedded in a CD access controls can be a reference point. Additionally, since regulations for computer viruses, spyware and the like cover several such legislative fields as information network security law, software law, copyright law and anti-circumvention law, anti-circumvention rules can be integrated with other laws to maximize their effectiveness.

To conclude, several Chinese laws and regulations have shown the effort that has been made to establish anti-circumvention rules that work effectively within an information network environment. The Copyright Act 1990 introduced a general anti-circumvention rule while the Software Regulation and the Network Regulation, particularly the latter, implemented a general rule with detailed provisions. The Supreme People's Court's judicial interpretation also has supplemented the legislative process. A comparison of the anti-circumvention rules in the DMCA, the CDPA and the Network Regulation shows that the Chinese anti-circumvention rules need continued expansion and updating with clarification and amendments.

A pragmatic approach is employed to develop anti-circumvention rules in diverse regulatory papers that follow the general guideline of the Copyright Act when dealing with such very different areas as software and the information network. Hence rules can to be formulated precisely and targeted. No facile modification should be made to the Copyright Act without adequate consultation and assessment. China needs to learn the necessary legislative techniques to construct its intellectual property law since the country has not had a modern such law.[114] China also needs time to identify and study its own economic and legal problems. A comprehensive understanding of China's real situation would help legislators to create tailored anti-circumvention rules rather than to blindly follow a western legal paradigm.

[1] For example, Universal City Studios, Inc. v Reimerdes 111 F. Supp. 2d 294, S.D.N.Y 2000 (henceforth Reimerdes). Eight major United States motion picture studios employed an encryption system called CSS (Content Scramble System) to protect the digital content of their DVDs, which contain copies of the motion pictures in digital form. CSS-protected motion pictures on DVDs may be viewed only on players and computer drives equipped with licensed technology that permits the devices to decrypt and play-but not to copy-the films. A computer program called DeCSS was designed to circumvent the CSS protection system and allowed CSS-protected motion pictures to be copied and played on devices that lack the licensed decryption technology. Defendants in the case quickly posted DeCSS on their Internet web site, thus making it readily available to much of the world.

2 For example, U.S. v Elcom Ltd 203 F. Supp. 2d 1111, 62 U.S.P.Q.2d 1736, 2002 Corp. L. Dec. P 28,453 (henceforth Elcom). A Russian programmer Dmitry Sklyarov designed a program to remove the security protections from Adobe eBook files. He was arrested in 2001 in the US. Adobe claimed it was tantamount to software piracy. See R Lemos "Russian's Arrest in Latest in Copyright Fight" at http://news.com.com.

3 L. Luo, "Legal Protection of Technological Measures - A Comparative Study of U.S., European, and Chinese Circumvention Rules", Hauser Global Law School Program working paper 08/05 at www.nyulawglobal.org at p. 6-7. A recent example occurred in late 2006, Jon Johansen, who is the designer of the DeCSS program and is famous for his work on reverse engineering data formats has again reverse engineered the Apple's FairPlay digital rights management technology. Although he claimed to have the permission from the Apple Company and thus is immune from the anti-circumvention liability, possible legal challenges from other companies is anticipated. See E. Oswald, "DVD Jon Opens up Apple's FairPlay" at www.betanews.com.

4 K. M. Hill, et al., "Digital Copyright and Public Policy" in Globalization of Intellectual Property in the 21st Century: Europe, Asia and the Internet, CASRIP Publication Series no. 5, 1999 at www-personal.umich.edu/~jdlitman. T. Ciro and M. Fox, "Competition & Copyright Protection in the Digital Age" (2006) EIPR 28(6) 329 at p. 334.

5"Metallica Sues Napster, Universities, Citing Copyright Infringement and RICO Violations" at www.livedaily.com ("From a business standpoint [trading files via Napster], this is about piracy--a.k.a. taking something that doesn't belong to you; and that is morally and legally wrong. The trading of such information--whether it's music, videos, photos, or whatever--is, in effect, trafficking in stolen goods," said Metallica drummer, Lars Ulrich). Content owners also attempted to use the legal process to arrest the development of digital copying technologies, see, e.g., UMG Recordings, Inc. v MP3.Com, Inc. 92 F. Supp. 2d 349 (S.D.N.Y.) 2000. Recording Industry Ass'n of Am., Inc. v Diamond Multimedia Systems, Inc., 29 F. Supp. 2d 624. *MGM Studios, Inc. v Grokster, Ltd.* 307F. Supp. 2d 1085 (N.D.Cal 2004) 125 S. Ct 2764, 2775 (2005).

[6] J. D. Lipton, "Solving the Digital Piracy Puzzle: Disaggregating Fair Use from the DMCA's Anti-device Provisions" (2005) 19 Harv. J. L. & Tech. 1, 111 at p.145 (It argues from a legislative perspective that the anti-trafficking and anti-device provisions in the DMCA and the CDPA would stifle individual legitimate use innovations). M. Kretschmer, "Digital Copyright: an End of an Era" (2003) EIPR 25(8) 333 at p.333. There is a possibility that computer code may replace law (another kind of code). See T. Wu, "When Code isn't Law" (2003) 89 Va. L. Rev. 679. J. C. Ginsburg, "Copyright and Control over New Technologies of Dissemination" (2001) 101 Colum. L. Rev. 1613. J. E. Cohen, "Some Reflections on Copyright Management Systems and Laws Designed to Protect Them" (1997) 2 Berkeley Tech L. J. 161, at p.161-162. J. Litman, "The Exclusive Right to Read" (1994) 13 Cardozo Arts & Ents L.J. 29.

[7] Luo, *op.cit*., p.5. S. Dusollier also argues that technology should not dictate what copyright law should look like, see "Technology as an Imperative for Regulating Copyright: From the Public Exploitation to the Private Use of the Work" (2005) EIPR 27(6) 201.

[8] Earlier, technological devices were not regulated under a copyright law regime based on a "technology neutral" principle that held the objective of regulation should be the information in use and not the devices or means by which the information is delivered or used. See H.R. Rep 105-551 (II) at p.24. For the first time art. 11 of WCT targeted acts of circumvention. The DMCA extended its reach from acts to devices and services as did the CDPA amendment. For comments, see T. B. Cohen, "Anti-circumvention: Has Technology's Child Turned against Its Mother?" (2003) 36 Vand. J. Transnat'l L. 961 at p. 973-975. P. B. Hugenholtz, "Software as a Commodity: International Licensing of Intellectual Property: Commentary: Copyright, Contract, and Code: What Will Remain of the Public Domain?" (2000) 26 Brooklyn J. Int'l L. 77 at p. 89.

[9] This legislative goal is expressed in a speech delivered by Cao Jianming, the Vice President of Supreme People's Court on the 6th Seminar on Trial of Intellectual Property Law at *www.chinaiprlaw.com/spxx/spxx108.htm*.

[10] Pub. L. No. 105-304, 112 Stat. 2860 (28 Oct 1998), relevant provisions codified at 17 U.S.C. §1201-1204. It amended title 17 of the US Code to extend the reach of copyright, while limiting the liability of internet service providers from copyright infringement by their users.

[11] Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 On the Harmonization of Certain Aspects of Copyright and Related Rights in the Information Society. OJ 2001 L 167/10.

[12] Copyright Law of the People's Republic of China (hereafter referred to as Copyright Act 1990). It was adopted in 1990 and amended in 2001.
[13] See subsection 4.1.
[14] Promulgated by Decree No. 468 of the State Council of the People's Republic of China, and effective as of 1 July 2006.
[15] Such as serial numbers and passwords.
[16] They are employed to protect videotapes, audio CDs, software and DVDs, etc. For example, Content Scrambling System (CSS) is used widely to protect unauthorized access and duplication of DVDs and Extended Copy Protection (XCP) is used to control production of CDs by Sony BMG Music.
[17] Digital rights management (DRM) is the umbrella term referring to any of several technologies used to enforce pre-defined policies controlling access to software, music, movies or other digital data. In more technical terms, DRM handles the description, layering, analyses, valuation, trading and monitoring of the rights held over a digital work. In its widest sense, the term refers to any such management. For a detailed description of major means of DRM, see above fn. 8, Cohen, at p. 973-974. For comments, see T. Vinje, "A Brave New World for Technical Protection Systems: Will There Still Be Room for Copyright?" (1996) EIPR 18(8) 431 at p. 431. Some commentators also suggest that the final resort of information protection relies on a variety of technologies, to name but a few, see C. Clark, "The Answer to the Machine is the Machine', Proceedings of Knowright '95 (1995). R. Poynder, *Caught in a Web-- Intellectual Property in Cyberspace* (Derwent / Thomson Scientific, 2001) at ch. 5. L. A. Hollaar, *Legal Protection of Digital Information* (BNA Books, 2002) at pp. 199-202.
[18] See *Religious Technology Center v Netcom On-Line Communication Services* 907 F. Supp. 1361, at 1370, it was ruled that "[T]he decentralized network was designed so that if one link in the chain be closed off, the information will be dynamically rerouted through another link."
[19] J. P. Liu, "Regulatory Copyright" (2004) 83 N.C.L. Rev. 87 at p. 129.
[20] P. Samuelson, "The Copyright Grab" (1996) *Wired*, issue 4.01 at *www.wired.com/wired/archive/4.01/white.paper_pr.html*.
M. Stefik, "In Internet Dreams: Archetypes, Myths, and Metaphors" in M. Stefik (ed.) *Letting Loose the Light: Igniting Commerce in Electronic Publication* (1996) at pp. 226-234. Also see M. Stefik "Shifting the Possible: How Digital Property Rights Challenge Us to Rethink Digital Publishing" (1997)12 Berkeley Tech. L. J. 137, at pp. 139-140. C. Clark, "The Publisher in the Digital World, in Intellectual Property Rights and New Technologies" Proceedings of the KnowRight '95 Conference at 85, pp. 97-101.
[21] J. Litman, *Digital Copyright*, (Prometheus Books 2001), at p. 27.
[22] See above fn. 6, Kretschmer, at p. 337. Also see above fn. 17, Vinje, at p. 436.
[23] For example, see art. I, s. 8 of Constitution of United States. Also see S. K. Stadler, "Forging a truly utilitarian copyright" (2006) 91 Iowa L. Rev. 609. In China, see art. 1, ch. 1 of Copyright Act 1990, English version available at *www.chinaiprlaw.com/english/laws/laws10.htm*. Preamble of WIPO Copyright Treaty (hereafter referred to as WCT), adopted in Geneva on December 20, 1996.
[24] Historically, copyright law reflected and responded to the advancements of technology. The invention of printing technology induced a nascence of copyright law, at least in the western world. For more discussions, see T. Dreier, "Developments and Perspectives of Copyright – From Gutenberg to Data Highway Proceedings of Kownright '95(1995). However, it is argued that the invention of printing appeared earlier in China, but China has not developed any law that was akin to copyright law, see W. P. Alford, *To Steal a Book is an Elegant Offense: Intellectual Property Law in Chinese Civilization* (Stanford University Press, 1995). Entering the electronic era, an innovative copyright levy system for remuneration collection and distribution for copyright holders was employed for such analog equipment, as the photocopy machine, and analog video and audio tape. More recently this has come to include such digital media and equipment, as hard disks. For more discussions, see P. Akester & R. Akester "Digital Rights Management in the 21st Century" (2006) EIPR 28(3) 159 at p. 159. Also see the report prepared by P. B. Hugenholtz, L. Guibault and S. Geffen on private copying levies, "The Future of Levies in a Digital Environment", March 2003, at *www.ivir.nl/staff/hugenholtz.html*. L. Guibault, "The Reprography Levies Across the European Union", March 2003, at *www.ivir.nl/staff/guibault.html*. Also see, e.g., *Sony Corp. of America v Universal City Studios*, 464 U.S. 417, 447 (1984) (Henceforth *Universal City Studios)*; *Teleprompter Corp. v Columbia Broadcasting System*, 415 U.S. 394 (1974); *Buck v Jewell-LaSalle Realty Co.*, 283 U.S. 191 (1931). The development of the multimedia network has inspired the creation of a new type of right – the "right of communication to the public", defined in art. 8 of WCT, entitles a copyright holder an exclusive right to distribute works in an "on-demand" format.
[25] Numerous papers contribute to the discussion and debate of the anti-circumvention rules. To name but a few, see P. Samuelson, "Intellectual Property and the Digital Economy: Why the Anti-circumvention Regulations Need to be Revised?"(1999) 14 Berkeley Tech. L. J. 519. P. Samuelson, "Anti-circumvention Rules Threaten Science" (2001) 293 Science 2028. L. Ginsburg, "Anti-circumvention Rules and Fair Use" (2002) UCLA L. J. Tech. 4. M. Hecht, "Reconciling Software and Anti-circumvention Provisions in the Digital Millenium Copyright Act" (2004)

UCLA L. J. Tech. 3. S. Lai, "The Impact of the Recent WIPO Copyright Treaty and Other Initiatives on Software Copyright in the United Kingdom" (1998) 1 IPQ 35 at pp. 42-61.
[26] WCT and WIPO Performances and Phonograms Treaty (hereafter referred to as WPPT) which was adopted in Geneva on December 20, 1996. They are together referred to as WIPO Treaties.
[27] See above, fn. 11.
[28] Copyright, Designs and Patents Act 1988.
[29] The Copyright and Related Rights Regulation 2003, SI 2003/ 2498.
[30] World Trade Organization, established in January 1, 1995, Geneva, created by Uruguay Round negotiations (1986-1994).
[31] Art. 58, ch. VI of Copyright Act 1990.
[32] Promulgated by Decree No. 339 of the State Council of the People's Republic of China, and effective as of 1 Jan 2002.
[33] Art. 24 of Software Regulation.
[34] Arts. 4, 18, 19 and 26 of ISP Interpretation.
[35] U. Gasser and M. Girsberger, "Transposing the Copyright Directive: Legal Protection of Technological Measures in EU-Member States" Berkman Publication Series No. 2004-10, at *http:// cyber. law. harvard. edu/ publication*s.
[36] S. 296 of CDPA.
[37] See above, fn. 6, Lipton, at p. 139.
[38] 17 U.S.C. § 1201. Also see US Copyright Office Summary of DMCA 1998, at pp. 3-4 (hereafter referred to as Summary) at http://www.copyright.gov/legislation/.
[39] 17 U.S.C. § 1201 (a) (3) (B).
[40] S. 296ZF of CDPA.
[41] S. 296ZF (2) of CDPA.
[42] See above, fn. 7, Dusollier, at pp. 202-203. D. L. Burk "Anticircumvention Misuse" (2003) 50 UCLA L. Rev. 1095, at p. 1096.
[43] See, e.g. *Reimerdes, Elcom* , *Lexmark Int'l* v S*tatic Control Components, Inc* 2003 U.S. Dist. LEXIS 3734 (E.D. K.Y 2003); 321 *Studios* v *Metro Goldwyn Mayer Studios, Inc* No.C 02-1955 SI (N.D. Cal 2004).
[44] 17 U.S.C. § 1201 (a) (1) (A).
[45] S. 296ZA 1(b) of CDPA, s. 296ZB(5) of CDPA.
[46] 17 U.S.C. § 1201 (a) (1) (A) and (a) (2). Also see above fn. 37, Summary at p. 3 and H.R. Rep I at p. 18.
[47] 17 U.S.C. § 1201 (b).
[48] S. R. Rep 105-190, S. Rep. No. 190, 105th Cong., 2nd Sess. 1998, 1998 WL 239623 at p. 29.
[49] Summary at p. 4. However, in *Universal City Studios, Inc.* v *Corley*, 273 F.3d 429, 443- 444, 60 U.S.P.Q.2d (BNA) 1953, 1961-1962 (2d Cir. 2001) it was ruled that the fair use defense was not applicable for circumvention over technological measures. Nevertheless, a different attitude was manifested in *Chamberlain Group, Inc.* v *Skylink Technologies, Inc.* (henceforth *Skylink)* 387 F.3d at 1178, 1204, 72 U.S.P.Q.2d (BNA) at 1225, 1244 (Fed. Cir. 2004). The Supreme Court ruled that the DMCA did not prohibit circumvention which did not constitute or facilitate copyright infringement. In *Skylink* 387 F.3d 522, at 546-549, 72 U.S.P.Q.2d (BNA) at 1839, 1856-1858 (6th Cir. 2004), the Sixth Circuit substantially diminished the purview of "access controls" protected by anti-circumvention and upheld the legality of circumvention for interoperability between competing products.
[50] S. 296ZB (1) (c) (iv), s. 296ZD (1) (b) (C) of CDPA.
[51] Only importing for private and domestic use is exempted explicitly in s. 296ZB (1) (b). According to the wording, of s. 296ZB (1) (c) (iv), possession in a course of business is prohibited.
[52] T. Heide, "Copyright in the EU and U.S.: What "Access Right?" 48 J Copyright Soc'y U.S.A. 363. L. N. Gasaway, "The New Access Right and Its Impact on Libraries and Library Users" (2003) 10 J. Intell. Prop. L. 269. J. C. Ginsburg, "From Having Copies to Experiencing Works: the Development of an Access Right in U.S. Copyright Law", Social Science Research Network Paper Collection at *http:// papers.ssrn.com/paper.taf?abstract_id=222493.*
[53] T. Vinje "The New Copyright Treaty: A Happy Result in Geneva" (1997) 19 EIPR 5, 230, at p. 235.
[54] Art. 11 of WCT.
[55] K. J. Koelman "A Hard Nut to Crack: the Protection of Technological Measures" (2000) 22 EIPR 6, 272, at p. 274.
[56] See subsection 3. 3.
[57] See *Reimerdes,* at 1891, 1900.
[58] 17 U.S.C. § 1201 (a) (2).
[59] S. 296ZD (1) (b) of CDPA.
[60] See *Universal City Studio*.
[61] D. L. Burk & J. E. Cohen, "Fair Use Infrastructure for Rights Management Systems" (2001) 15 Harv. J. L. &

Tech. 41, at pp. 46-47. Lobbyists claimed that the *Sony* substantial non-infringing standard was insufficient for copyright protection, see "Online Copyright Liability Limitation Act: Hearing before the Subcommittee on Courts and Intellectual Property of the Committee on the Judiciary", 105th Cong. (1997) (hereafter referred to as The Hearing 1997) at p. 33 (statement of M Peters, Register of Copyrights, Copyright Office of the United States).

[62] 17 U.S.C. § 1201 (c) (1).

[63] They are (1) a non-profit library, archive, and educational institution; (2) reverse engineering; (3) encryption research; (4) minor protection; (5) personal privacy and (6) security testing.

[64] 17 U.S.C. § 1201 (a) (1) (B)-(E).

[65] For an evaluation of this exemption, see W. N. Hartzog, "Falling on Deaf Eras: Is the Fail-Safe Triennial Exemption Provision in the Digital Millenium Copyright Act Effective in Protecting Fair Use?" (2005) 12 J. Intell. Prop. L. 309.

[66] Library of Congress "Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies" vol. 71, no. 227, pp. 68472-68480 at *www.copyright.gov/ fedreg/2006/71fr68472.html*.

[67] They are computer programmes protected by obsolete dongles (a dongle is a small hardware device that connects a computer to authenticate some piece of software); computer programmes and video games distributed in obsolete formats and eBooks without read-aloud functions or prevent users from converting the text into another format.

[68] They are audiovisual works in a university film archive; firmware on mobile telephone handsets and sound recordings on CDs protected by access controls that create security vulnerabilities.

[69] See *www.eff.org/IP/DRM/Sony-BMG*.

[70] See subsection 4.1.

[71] The permitted acts are enumerated in Pt. 1 of Sch. 5A of CDPA.

[72] P. Samuelson, "Towards More Sensible Anti-circumvention Regulations" part IV, at *www.sims.berkeley.edu/~"pam/papers/fincrypt2.pdf*. P. Samuelson, "Intellectual Property and Digital Economy: Why the Anti-circumvention Regulations Need to be Revised" (1999) Berkley. Tech. L. J. 519, at pp. 544 -546.

[73] Senator O. G. Hatch, "Toward A Principled Approach to Copyright Legislation at the Turn of the Millennium" (1998) 59 U. Pitt. L. Rev. 719, at pp. 749-750 .

[74] The Hearing 1997 at pp. 78-82. (statement of Jack Valenti, President and CEO, Motion Picture Ass'n of America); id. at pp. 256-265 (statement of Edward J. Black, President, Computer and Communications Industry Ass'n). The Business Software Alliance, whose principal member is Microsoft, supported Hollywood's preferred bill basically because of the "trusted system" which makes uses or copies of protected works very difficult or impossible by a cooperated system between computer and software. For details, see above fn. 37, Samuelson, footnotes 180-186 and accompanying text. I. R. Kerr, A. Maurushat and C. S. Tacit, "Technological Protection Measures: Tilting at Copyright's Windmill" (2002) 34 Ottawa L. Rev. 7 32 at p. 32.

[75] See US Dep't of Commerce Info. Infrastructure Task Force, Intellectual Property and the National Information Infrastructure: The Report of the Working Group on Intellectual Property Rights (1995) (hereinafter White Paper). Numerous articles have criticized this and an earlier draft report because of its imbalance that was heavily in favor of publisher interests. See, e.g., P. A. Jaszi, "Caught in the Net of Copyright" (1996)75 Or. L. Rev. 299; L. Kurtz, "Copyright and the National Information Infrastructure" (1996)18 EIPR 120; J, Litman, "The Exclusive Right to Read" (1994) 13 Cardozo Arts & Ent. L. 29. See above fn. 19, Samuelson, at 134. Also see P. Samuelson, "The US Digital Agenda at the WIPO" (1997) 37 Va. J. Int'l L. 369. It discussed the negotiations that led to the conclusion of the WCT.

[76] See above fn. 71, P Samuelson, "Towards More Sensible Anti-circumvention Regulations" at p. 7.

[77] For example, see *Davidson & Associates v Jung* 422 F.3d 630, 2005 Copr.L.Dec. P 29,043, 76 U.S.P.Q.2d 1287

[78] S. A. Shayesteh "High Speed Chase on the Information Superhighway: the Evolution of Criminal Liability for Internet Piracy" (1999) 33 Loy. L.A. L. Rev 183, at pp. 213-216, 223-224.

[79] Art. 11 of WCT and art. 18 of WPPT.

[80] See above fn. 34, the closing remarks of "Transposing the Copyright Directive" at p. 30, in which the legal protection of technological measures on both sides of the Atlantic are regarded as not being a prime example of legislation.

[81] See above fn. 10.

[82] For a comprehensive comparison among several jurisdictions including the WCT, US, EU, Japan and Australia, see R. Wang, "Ant-circumvention Provisions in a Different Light: Perspectives from Transnational Observation of Five Jurisdictions (2006) 34 AIPLA O.J. 217.

[83] K. Hu, "The Modernization of Intellectual Property System in the Development of High Technologies" (2005) 5 *Studies in Law and Business* 7, at p. 8. (胡开忠 "高新技术发展中的知识产权制度现代化" 《法商研究》第5期, 2005年) Also see an interview about issues of software protection by Mr. G Tang, Chief Secretary of Intellectual Property Law Center, China Academy of Social Science, at *www.chinaiprlaw.cn/file/200507315370.html.* He is concerned about the absence of concrete anti-circumvention rules that can curb the technological measures'

negative impact on consumers and users.
[84] See a distributor's report at *www.law-lib.com/flsz/sz_view.asp?no=1198*.
[85] X. Zhang "Studies on Several Issues Concerning the Intellectual Property Protection in the Network Environment" at *http://218.69.114.37/wf/~CDDBN/Y690131/PDF/index.htm* at pp.16-17. (张晓宇, "互联网络中知识产权保护的若干问题研究").
[86] J. Yang, et al, "Why KV300L++ Anti-virus Software is Illegitimate and the Possibility of the Implementation of 'Self-defence' of Software Copyright Protection—A Discussion from Over Defence by the KV300L++ Anti-virus Software" (1998) 3 *Copyright* 36 at *www.usstec.com/info/041025kv300.doc*. (杨坚争、辛琳、陈红梅、吕国恒 "KV300L++版反病毒软件的违法原因与软件版权保护中实施 '正当防卫' 的可能性——从KV300L++版反病毒软件的防卫过当谈起"《著作权》1998年第3期36). B. Shou "Reflection and Analysis on the Software's Logic Bomb Case" *Beijing International Electronic Newspaper*, August 12, 1997. (寿步 "软件逻辑炸弹一案的反思与分析"北京《国际电子报》1997-08-12) "Where is the Boundary of the Technological Protection – A Discussion from KV300 Software Logic Bomb" at *http://tech.sina.com.cn/it/e/2001-12-23/97046.shtml* ("技术保护，界限何在—从KV300软件逻辑炸弹案谈起"）
[87] Approximately equivalent to €500.
[88] T. Liao, "KV300L++ 'Logic Lock' Has A Conclusion—Beijing Municipal Public Security Bureau Decided to Impose Administrative Penalty" *Chongqing Computer Newspaper*, September 12, 1997. (廖天华 "KV300L++'逻辑锁'事件有结论——北京市公安局作出行政处罚决定" 重庆《电脑报》1997-09-12。)
[89] It incorporated the substantive provisions of the Berne Convention and is administrated under the WTO.
[90] The Chinese intellectual property legal system is comprised of three parts: laws, administrative regulations and special department rules. Judicial interpretations are supplementary. For an introduction of Chinese IP law, see "Intellectual Property Protection in China" at *www.chinaiprlaw.com/english/news/news46.htm*.
[91] Berne Convention for the Protection of Literal and Artistically Works, first established in 1886 and recently amended in 1979
[92] For example, see *Shanghai Busheng Music and Culture Broadcast Ltd. v Baidu Tech Ltd.*, case number 14665 of first instance Haidian District Court (2005)
(上海步升音乐文化传播有限公司诉百度网讯科技有限公司，海民初字第14665号). Without clear regulation of the standards of the inducement of ISPs' liability, Baidu, a search engine company which has provided links to free MP3 download, was sued by the Shanghai Busheng Ltd, a music production company, of copyright infringement. Baidu lost the case and paid fine to Shanghai Busheng Ltd.
[93] http://www.gov.cn/zwhd/2006-05/29/content_294127.htm. (Chinese version only)
[94] Art. 26 of Network Regulation.
[95] *ibid*.
[96] See above fnn. 61-63 and accompanying text.
[97] Art. 4 of Network Regulation.
[98] Art. 4 in general and arts. 8 and 19 in particular.
[99] Some commentators argued that the *scienter* requirement would impose copyright and neighboring rights holders an unreasonable burden of proof to show the intention of an infringing party. Moreover, it may encourage others to circumvent technological measures. See above fn. 94, Zhang at p. 123.
[100] J. Y. Zhang, "Copyright Owners' Rights over the Internet" (2006) 9 *China Law & Practice* 80.
[101] See above fn. 102.
[102] Art. 12 of Network Regulation.
[103] The sole purpose approach was also proposed by Singapore in the ""Basic Proposal for the Substantive Provisions of the Treaty on Certain Question of Literary and Artistic Works to be Considered by the Diplomatic Conference" WIPO Doc. CRNR/DC/12 (1996) at *www.wipo.int/documents/en/diplconf/distrib/pdf/12dc.pdf*.
[104] See above fn. 24, Lai, at p. 47.
[105] J. H. Blavin summarized "that copyright statutes are inherently bent in favor of status quo interests and biased against absent interests (e.g., the public), thus resulting in inflexible laws that lack of long-term stability as new technologies emerge". This is in Litman's *Digital Copyright*, at 62 in his book note "*Digital Copyright* - by Jessica Litman Amherst, NY: Prometheus Books" (2001) 14 Harv. J. L. & Tech. 741, at p. 745. To avoid this myopic legislative trend, there should be a general exception in the Chinese anti-circumvention rules that will give the law more flexibility to accommodate future technological innovation and thus have legal stability.
[106] See above fn. 93, Cao, at p.11.
[107] Art. 12 (1) of Network Regulation.
[108] The importance of reverse engineering are analyzed in T. Vinje, "Threat to Reverse Engineering Practices Overstated" (1994) EIPR 16(8) 364 and also in above fn. 16, Vinje, "A Brave New World for Technical Protection Systems" at p. 437. Also see *Sega Enterprises, Ltd v Accolade, Inc*. 977 F. 2d 1523- 1524 (9th Cir. 1992) in which

the Court noted that decompilation techniques are widely used in the software industry, and stated that "an attempt to monopolize the market by making it impossible for others to compete runs counter to the statutory purpose of promoting creative expression".

[109] *Felton v RIAA* [US DC NJ Case # CV-01-2669 (GEB)] is a referential case to this point. A team of researchers led by Professor Felton participated in a public event called Hack SDMI Challenge. Having learned that they would present a paper explaining their discovery that the SDMI (Secure Digital Music Initiative) technology was insecure and would be defeated upon its introduction to the public, the Recording Industry Association of America (RIAA) composed a letter threatening legal action under the DMCA if they present their discovery. Fearing the legal liability, the scientists withdrew their paper from the Conference. For comment on this case, see R. D. Gross, "Digital Millennium Dark Ages: New Copyright Law Used to Threaten Scientific Research" November 7, 2001 at *www.eff.org/IP/DMCA/Felten_v_RIAA/20011107_eff_felten_article.html*. To avoid the same chilling effect from happening again the anti-circumvention rules may create an exception for the circulation and communication of research results within an academic community that is reasonable.

[110] Although it is criticized as ''formalistic" in language, see J. Deng, "The Supreme People Court's Take On Copyright Liabilities for ISPs" (2004) 18 *China Law and Practice* (3).

[111] See above fn. *59*, *Universal City Studios*, the Supreme Court held that the sale of copying equipment does not make one liable for direct infringement, even when one had the constructive knowledge that purchasers may use it for an infringing purpose. In *Fonovisa, Inc. v Cherry Auctions, Inc.*, 76 F.3d 259, 264 (9th Cir. 1996), contributory infringement involves situations in which one has knowledge of the infringement and materially contributes to it. Vicarious infringement deals with the situation where one has a financial interest in, and the right to supervise,the infringement.

[112] In the US, the passivity doctrine is applied if an ISP has not been actively involved in an infringing act. Then the ISP could be exempted from liability. See *Religious Technology Center v Netcom On-Line Communication Services, Inc.* 907 F. Supp. 1361 (N.D. Cal. 1995) and *CoStar Group, Inc*. v *LoopNet, Inc*. 373 F.3d 544 (4th Cir. 2004), DMCA also protects ISPs from direct liabilities by the passivity doctrine, see 17 U.S.C. § 512. For comments, see B. W. Barger, Jr. "*CoStar* v *LoopNet*: Protection of the Internet at the Expense of Copyright Protection?" (2006) 6 Chi.-Kent J. Intell. Prop 1. A passivity doctrine also can be considered in Chinese anti-circumvention rules in deciding ISPs' liabilities in providing circumventing technology or devices. This doctrine can relieve ISPs of the burden of scrutinizing, and thus encourage the development of the Internet.

[113] "Safe harbor" principle only applies strictly to ISPs, see art. 2 of Administrative Protection Measures of Copyright via Internet 2005.

[114]Alford, *To Steal a Book is an Elegant Offense*, (1995). However, some Chinese scholars argue that China has its own law akin to copyright in the pre-modern Chinese culture, see K. Shao, "An Alien to Copyright? A Reconsideration of the Chinese Historical Episodes of Copyright" (2005) 4 IPQ 400. For a detailed analysis on the Chinese ancient legal system with particular reference to copyright law from the invention of printing to the time prior to 1949 (the year when the People's Republic of China was founded), see C. Zheng and M. Pendleton, *Copyright Law in China* (CCH International, 1991), at pp. 9-17; for a more comprehensive introduction that covers the evolution of Chinese copyright law until 1990, see *ibid*. at pp. 17-66.