

Maurer School of Law: Indiana University

Digital Repository @ Maurer Law

Theses and Dissertations

Student Scholarship

11-2016

Evaluating the Legal Issues of Internet Service Providers in China – A Comparative Copyright Analysis of Chinese ISPs, the U.S. ISPs, and Japanese ISPs

Yifan Huang

Indiana University Maurer School of Law, raphael.huang@hotmail.com

Follow this and additional works at: <https://www.repository.law.indiana.edu/etd>



Part of the [Comparative and Foreign Law Commons](#), and the [Intellectual Property Law Commons](#)

Recommended Citation

Huang, Yifan, "Evaluating the Legal Issues of Internet Service Providers in China – A Comparative Copyright Analysis of Chinese ISPs, the U.S. ISPs, and Japanese ISPs" (2016). *Theses and Dissertations*. 33.

<https://www.repository.law.indiana.edu/etd/33>

This Thesis is brought to you for free and open access by the Student Scholarship at Digital Repository @ Maurer Law. It has been accepted for inclusion in Theses and Dissertations by an authorized administrator of Digital Repository @ Maurer Law. For more information, please contact rvaughan@indiana.edu.



JEROME HALL LAW LIBRARY

INDIANA UNIVERSITY
Maurer School of Law
Bloomington

**EVALUATING THE LEGAL ISSUES OF INTERNET SERVICE PROVIDERS
IN CHINA –A COMPARATIVE COPYRIGHT ANALYSIS OF
CHINESE ISPS, THE U.S. ISPS, AND JAPANESE ISPS**

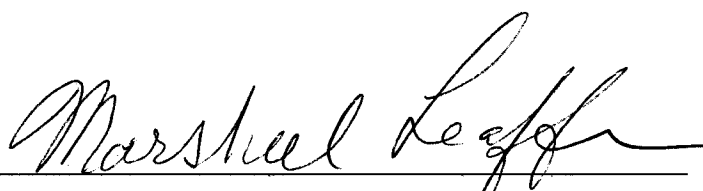
YIFAN HUANG

Submitted to the faculty of Indiana University Maurer School of Law
in partial fulfillment of the requirements
for the degree
Master of Laws – Thesis

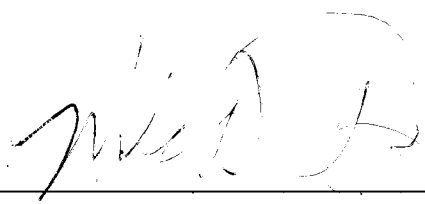
November 2016

Accepted by the faculty, Indiana University Maurer School of Law, in partial fulfillment of the requirements for the degree of Master of Laws – Thesis.

Thesis Committee



Marshall A. Leaffer



Mark D. Janis

November 2016

Updated September 2011

TABLE OF CONTENTS

CHAPTER I	1
INTRODUCTION	1
A. BACKGROUND.....	1
B. ISP ISSUE IN CHINA.....	2
C. OVERVIEW.....	3
CHAPTER II	5
ABOUT ISP AND UGC	5
A. THE DEFINITION OF ISP	5
1. <i>International treaties</i>	5
2. <i>The U.S. Law</i>	6
3. <i>Japanese Law</i>	6
4. <i>Chinese Law</i>	6
5. <i>Comparative methodology</i>	7
B. A NEW BUSINESS MODEL - USER GENERATED CONTENT SERVICE	7
1. <i>The “Safe harbor” doctrine and the “notice and takedown” provision</i>	8
2. <i>User Generated Content</i>	8
3. <i>Legal issue in China</i>	9
CHAPTER III	11
APPROACH TO ISPS’ COPYRIGHT LIABILITY IN THE U.S.	11
A. HISTORICAL CONTEXT OF ISP’S COPYRIGHT LIABILITY	12
1. <i>Background</i>	12
2. <i>Direct Infringement</i>	13
3. <i>Secondary Liability</i>	13
4. <i>Contributory Liability</i>	14
5. <i>Vicarious Liability</i>	14
B. SECTION 512 OF THE DMCA AND SAFE HARBOR.....	15
1. <i>The Online Copyright Infringement Liability Limitation Act (OCILLA)</i>	15
2. <i>Section 512(c)-(d)</i>	15
C. ISP’S COPYRIGHT LIABILITY ESTABLISHED BY COMMON LAW CASES	16

1. <i>Sony Safe harbor rule</i>	16
2. <i>Inducement theory</i>	17
D. CASES.....	17
1. <i>American Broadcasting Cos. v. Aereo, Inc.</i>	18
2. <i>Viacom v. Google/YouTube</i>	23
CHAPTER IV.....	29
CHINESE AND JAPANESE APPROACH TO ISP'S COPYRIGHT LIABILITY.....	29
A. CHINA'S NEW APPROACH TO ISPS' COPYRIGHT LIABILITY.....	30
1. <i>New Developments in ISP Copyright Liability in China</i>	30
B. CASE: <i>CHINA YOUTH PUBLISHING GROUP V. BAIDU WENKU</i> ,.....	37
1. <i>Background</i>	37
2. <i>The Plaintiff's Claims</i>	38
3. <i>The Defendant's Defense</i>	39
4. <i>The Court's Decision</i>	39
5. <i>"Should have known" rule</i>	41
6. <i>ISP's reasonable duty of care</i>	44
7. <i>Paradox for ISP</i>	46
C. JAPAN'S NEW APPROACH TO ISPS' COPYRIGHT LIABILITY.....	48
1. <i>Statutes</i>	48
2. <i>Case: Winny</i>	50
3. <i>The Japanese Supreme Court's opinion on Winny</i>	51
4. <i>Inducement analysis</i>	54
5. <i>Summary</i>	55
CHAPTER V.....	56
COMPARATIVE ANALYSIS: THE U.S., CHINA, AND JAPAN.....	56
A. SIMILARITIES AMONG THE U.S., CHINA AND JAPAN.....	56
B. THE DIFFERENCE BETWEEN THE U.S., CHINA AND JAPAN.....	58
1. <i>Different ISP approach - passive-reactive vs. active-preventive</i>	58
2. <i>Different legal systems – common law vs. civil law</i>	61
3. <i>The active-preventive trend in China</i>	62
C. THE POTENTIAL PROBLEMS LURKING IN THE ACTIVE-PREVENTIVE ISP MODEL.....	63

1. <i>Definition of ISP</i>	63
2. <i>Legal conflict</i>	65
CHAPTER VI	66
ALTERNATIVE SOLUTIONS	66
A. “STANDARD TECHNICAL MEASURE” EXCEPTION.....	66
1. <i>Section 512 (i)</i>	66
2. <i>Reasonable duty of care</i>	67
B. THE GRADUATED RESPONSE.....	67
1. <i>Historical context</i>	67
2. <i>ISP</i>	69
3. <i>The Graduated Response procedure from the U.S.</i>	72
C. A TECHNICAL SOLUTION	73
CHAPTER VII	76
CONCLUSION	76

ACKNOWLEDGMENTS

This thesis will form the foundation of my SJD dissertation for the next three years. I could not have finished it without the guidance and help of many people.

First, I have to express my sincere gratitude to my supervisor, Professor Marshall A. Leaffer, for being a great mentor and advisor. He taught me the most important aspect of writing an academic article: communicating with your readers; always consider what your readers would think about when they are reading your article, help your readers to understand your opinions, show your readers why your opinions are important to your article. These points are extremely helpful for academic writing.

In addition, I would like to express my deepest thanks to my friend, Kimberly Wright for her detailed review throughout this thesis. As a foreigner student, I am not able to finish my thesis without her generous help and proofreading.

My special thanks go to Dean Lesley Davis who helped me overcome the serious health condition I faced when I extracted my wisdom teeth.

Last but not least, I want to thank all the tutors from Wells Library who helped me review my thesis. Also, thanks to all my family members for supporting my academic career in the U.S.

黄一帆

November 2016

ABBREVIATION GUIDE

CATV: community antenna television

Creation and Internet Act: Law Promoting the Distribution and Protection of Creative Works on the Internet

CNNIC: China Internet Network Information Center

DMCA: Digital Millennium Copyright Act

DRM: digital rights management ()

EU: European Union

FCC: Federal Communications Commission

HADOPI: High Authority for the Dissemination of Works and the Protection of Rights on the Internet

IAP: Internet apparatus provider

ICM: Measures for the Administrative Protection of Internet Copyright Measures

ICP: Internet content provider

IP: Intellectual Property

ISP: Internet Service Provider

IU: Indiana University

Judicial interpretation: the Supreme People's Court's interpretation

Kao's Diary: Kao La Xiao Wu's English Learning Diary

Limitation of Provider liability Act: act on the Limitation of Liability for Damages of Specified Telecommunications Service Providers and the Right to Demand Disclosure of Identification Information of the Senders

MD5: MD5 Message-Digest Algorithm

MII: Ministry of Information Industry

NCA: National Copyright Administration

OCILLA: Online Copyright Infringement Liability Limitation Act

The Provision: Provisions of the Supreme People's Court on Several Issues concerning the Application of Law in Hearing Civil Dispute Cases Involving Infringement of the Right of Dissemination on Information Networks

P2P: peer-to-peer

P2PTV: Peer-to-Peer Assisted Streaming Television

PRC: People's Republic of China

RCI Regulation: Regulations for the Protection of the Right of Communication through Information Network

Right of dissemination through information network: the right to communicate works to the public over information networks

RS-DVR: Remote Storage Digital Video Recorder system

TPMs: technological protection measures

TRIPS Agreement: Agreement on Trade-Related Aspects of Intellectual Property

UGC: User Generated Content

U.S.: United States

VPN: virtual private network

WCT: WIPO Copyright Treaty

WIPO: World Intellectual Property Organization

ABSTRACT

This thesis is motivated by a legal challenge in the area of Chinese copyright protection: Baidu, which was considered a disaster by the copyright owners in China. To solve this legal challenge, the Chinese could learn from the legal experience of Japan and the U.S. regarding this issue.

The traditional ISP legal system provides a passive-reactive approach to the secondary copyright liability of ISPs. However, the Baidu issue in China indicates that a passive-reactive ISP model is not able to prevent copyright infringement. Recent cases in China and the U.S. reflect a new trend that the judicial branch adopts an active-preventive approach to ISP issues. This thesis organizes the various legal theories, statutes and cases that may be relevant in an ISP dispute into a framework that may be used to more clearly and effectively evaluate the legal issues of ISPs, with a focus on the proposal for Chinese copyright legal reform.

This thesis consists of two parts. The first part examines ISP-related law and cases in the U.S., China and Japan. The second part comparatively analyzes the Baidu issue and suggests possible solutions for Chinese legislature.

Chapter I

Introduction

A. Background

The Internet world has no geographic boundary. As such, how to determine the liability of Internet Service Providers (ISPs) between different jurisdictions has become one of the global issues in Internet and Intellectual Property (IP) law. In the digital network world, each individual can make copies of the original digital work and distribute it through the network. With the development and popularization of network technology, an Internet user can easily get access to a copyright work, or make a copyright work available through network to the public without the authorization of the copyright owner. As a result, an ISP can easily involve in copyright infringement for the infringing material occurring on their network. The copyright owners usually demand strong protection on their copyright works, while most of the Internet users would like to access online materials for free. As an intermediary, whether ISPs should actively protect copyright work is a controversial problem. Therefore, it is necessary to consider how to balance the interests among Internet users, ISPs and copyright owners.

Different countries have different approaches to address this issue. As one of the most developed countries in network technology, the United States (U.S.) has established a complete legal theory about direct and secondary liability of ISPs. Other countries, such as China¹ and Japan, have followed the U.S. safe harbor model to regulate the copyright liability of ISPs.² However, they did not just transplant the ISPs liability model from the U.S. In accordance with their own legal environments, they enacted different ISP provisions in

¹ The term "China" in this paper refers to the jurisdiction of mainland China ("People's Republic of China")

² JEREMY DE BEER & CHRISTOPHER D. CLEMMER, *Global Trends in Online Copyright Enforcement: A Non-Neutral Role for Network Intermediaries?*, 49 JURIMETRICS J. 375, 377-378 (2009).

order to meet local conditions.

B. ISP issue in China

In China, copyright infringement has been a serious issue and most of its recent copyright cases are related to ISPs. For example, from 2011 to 2014, “Baidu Ltd”, a Chinese tech company, similar to “Google” in the U.S., has repeatedly been sued more than 40 times for copyright infringement.³ In the area of literary works, Baidu was accused of copyright infringement by the Chinese author group, Music Copyright Society of China, Cloudary Corporation⁴, and even China Central Television.⁵ In the area of film, Baidu was also accused of copyright infringement by the China Film Copyright Association, Wanda Media Co. Ltd, and the Motion Picture Association of America.⁶

Most of the cases are related to Baidu’s User Generated Content (UGC) services, such as Baidu Wenku or Baidu Cloud. Although Baidu lost almost all of their copyright infringement lawsuits, the copyright owners can do nothing to prevent Baidu from copyright infringement again.⁷ As a result, for many copyright owners, “Baidu” is a disaster in the IP protection area.⁸ Moreover, the other ISPs in China, such as “Alibaba” and “Tenxun,” are also involved in the same copyright infringement issues. This thesis considers Baidu as a typical example of ISP in China and discusses the solution to improve issues involving ISPs and copyright infringement.

³ Zhang Yanhong (张艳红), *China Youth Publishing Group sue Baidu and win on the court of first instance* (中国青年文库诉百度一审胜诉), *Electronics Intellectual Property* (电子知识产权), Z1-2015, at 29.

⁴ Digital publishing company Cloudary Corporation was incorporated by Shanda Group in Jul 2008, creating the world’s largest Chinese- language original content platform. SHANDA, <http://www.shanda.com/about-us> (last visited Oct 18, 2016).

⁵ CCTV is an official media company operated by Chinese government. CCTV, <http://english.cctv.com/> (last visited Oct. 18, 2016).

⁶ Zhang, *supra* note 3, at 28.

⁷ *Id.* at 29.

⁸ *Id.*

These problems in China reflect the imbalance among copyright owners, Internet users and ISPs. Therefore, the primary task for Chinese legislature is to figure out a better ISP model for the purpose of copyright protection. This thesis analyzes why the current regulations of ISPs in China are not able to provide complete protection to copyright owners, and suggests some solutions about how to solve this issue by comparing the ISP policy from Japan and the U.S.

C. Overview

Recent ISP cases in the U.S. and China demonstrate a trend from a passive-reactive approach toward an active-preventive approach.⁹ However, as a civil law jurisdiction near China, Japan has not followed this trend. Nevertheless, the experience from these two jurisdictions provides new insight into how China can reform its own ISP policy. The purpose of this thesis is to analyze the ISP issues in China by comparing statutes and cases in the U.S. and Japan, and to suggest legal reform that will balance the interests among ISPs, Internet users and copyright owners. Taking into consideration recent copyright cases in China, this thesis discusses the legal issue of current ISP models in China and suggests that Chinese legislature should reform the ISP protection from a passive-reactive model to an active-preventive model for the purpose of better copyright protection.

This thesis consists of six chapters. Chapter II introduces the background and scope of this thesis, and presents how the comparative methodology will be used to analyze and develop issues in this thesis. Chapter III of this article focuses on the copyright liability theories of ISPs in the U.S., and some famous ISP cases including the *American*

⁹ JEREMY & CHRISTOPHER, *supra* note 2, at 375.

*Broadcasting Corp. v. Aereo (Aereo)*¹⁰ case, which was decided by the U.S. Supreme Court in 2014. Chapter IV discusses the copyright law regime in China and Japan, and then examines two milestone cases in these two countries: the *China Youth Publishing Group v. Baidu Wenku (Baidu)*¹¹ case, which is the first lawsuit involving a publisher against Baidu Wenku in China, and the *Japan v. Winny (Winny)*¹² case, which is the first contributory infringement peer-to-peer (P2P) case in the Japanese Supreme Court. Chapter V turns to a comparative analysis of the similarities and differences between China, Japan and the U.S., and then addresses problems and uncertainty under PRC law of ISPs' secondary liabilities. To solve these issues, this chapter suggests Chinese legislature should reform the ISP protection from a passive-reactive model to an active-preventive model. Chapter VI further discusses the flaws of the current Chinese law of ISP liability and proposes some recommendations and solutions to be considered in the future.

¹⁰ American Broadcasting Corp. v. Aereo, 134 S.Ct. 2498 (2014).

¹¹ Běijīng zhōng qīng wén wénhuà chuánméi yǒuxiàn gōngsī děng zhùzuòquán quán shǔ, qīnquán jiūfēn èrshēn mínshì pàn jué shū (北京中青文文化传媒有限公司等著作权权属、侵权纠纷二审民事判决书) [*China Youth Publishing Group v. Baidu Wenku*], 2014 Gao Min Zhong Zi No. 2045 (Beijing High People's Ct. Aug 5, 2014).

¹² Saika Saibansho [Sup. Ct.] Dec. 19, 2011, 2009 (A) No. 1900, 65 SAIKO SAIBANSHO KEIJI HANREISHU [KEISHU] 1, <http://www.courts.go.jp/hanrei/pdf/20111221102925.pdf>. The Court's English translation can be accessed at <http://www.courts.go.jp/english/judgments/text/2011.12.19-2009.-A-.No..1900.html>.

Chapter II

About ISP and UGC

This chapter introduces the definition of ISP in the U.S., China and Japan, and the methodology this thesis will use to comparatively analyze legal materials from different jurisdictions in order to conclude an appropriate proposal for legal reform. From a technical perspective, this chapter explains what is UGC and why it relates to most of the recent ISP cases in the U.S. and China.

A. The Definition of ISP

1. International treaties

The World Intellectual Property Organization (WIPO) Internet Treaties are considered the first international agreements to deal with copyright issues in the digital network world. Although there is no specific liability regulation for ISP, Article 8 of WIPO Copyright Treaty (WCT) grants copyright owners “the exclusive right of authorizing any communication to the public of their work, by wire or wireless means.”¹³ Any activity that makes copyright work available to the public, without authorization by the copyright owner, is considered copyright infringement. To restrict these exclusive rights of the copyright owner from overexpression, The agreed statement concerning Article 8 of WCT precludes “that the mere provision of physical facilities for enabling or making a communication does not in itself amount to communication within the meaning of this Treaty . . . ” provides a safe harbor for a network intermediary such as an ISP.

¹³ WIPO Copyright Treaty, art. 8.

2. The U.S. Law

In the U.S., the Digital Millennium Copyright Act (DMCA) was enacted on Oct. 28, 1998. Section 512(k)(1) of the DMCA stipulates two definitions of ISP, one narrow and one broad. Section 512(k)(1)(A), which is the narrow one, only applies to ISP that falls under Section 512(a). The broad definition of ISP under Section 512(k)(1)(B) means “a provider of online services or network access, or the operator of facilities therefor, and includes an entity described in subparagraph (A).”¹⁴ This thesis adopts the broad definition of ISP under Section 512(k)(1).¹⁵

3. Japanese Law

The “act on the Limitation of Liability for Damages of Specified Telecommunications Service Providers and the Right to Demand Disclosure of Identification Information of the Senders” (Limitation of Provider liability Act) was enacted on November 30, 2001. Article 2 (iii) of the act defines “specified telecommunications service provider” (ISP) as “a person who relays others' communications [sic] with the use of specified telecommunications facilities, or provides specified telecommunications facilities to be used for others' communications [sic].”¹⁶ This is a broad definition compared to the U.S. law.

4. Chinese Law

In China, one of the legal issues involving ISP is that although there are many laws

¹⁴ 17 U.S.C. § 512(k)(1)(B).

¹⁵ ISP also define as “an entity offering the transmission, routing, or providing of connections for digital online communications, between or among points specified by a user, of material of the user's choosing, without modification to the content of the material as sent or received.” See 17 U.S.C. § 512(k)(1)(A).

¹⁶ Tokutei denki tsūshin ekimu teikyō-sha no songai baishō sekinin no seigen oyobi hasshinsha jōhō no kaiji ni kansuru hōritsu [Purobaida sekinin seigen-hō] [Act on the Limitation of Liability for Damages of Specified Telecommunications Service Providers and the Right to Demand Disclosure of Identification Information of the Senders (Limitation of Provider liability Act)] Act No. 137 of 2001, art. 2, para. 3 (Japan). English translation are available at <http://www.japaneselawtranslation.go.jp/law/detail/?id=2088&vm=04&re=01&new=1>.

and regulations, there is no specific definition for an ISP in any Chinese legal codes. Article 14 of the Regulations for the Protection of the Right of Communication through Information Network (RCI Regulation) stipulates that “for a network service provider that provides information storage space or provides searching and linking services . . .”¹⁷ is only an illustration of an ISP rather than a definition. This lack of definition may cause huge uncertainty for legal liability. Therefore, many scholars in China try to define ISP from an academic perspective.¹⁸ By comparing the ISP definition in the U.S., Japan, and Chinese case law, this thesis analyzes the lack of ISP definition in China and provides a legal proposal that China should adopt a broad definition for ISPs in Chapter V.

5. Comparative methodology

This thesis will analyze the lack of ISP definition and provide suggestions for legal reform by a comparative methodology in Chapter V. In addition, the same methodology will also be used to analyze ISP models in China, Japan and the U.S. As a conclusion of the analysis, this thesis suggests that Chinese legislature should reform the ISP protection from a passive-reactive model to an active-preventive model by comparing the ISP legal model in Japan and the U.S.

B. A New Business Model - User Generated Content Service

¹⁷ Xin xi wang luo chuan bo quan bao hu tiao li (信息网络传播权保护条例) [Regulations for the Protection of the Right of Communication through Information Network] (promulgated by the St. Council, May 18, 2006, amended by the St. Council in Jan 30, 2013) art. 14 (China). The English translation is available at <http://www.cpahkltd.com/UploadFiles/20100315165559735.pdf>.

¹⁸ Luo Yong (罗勇), *Legal definition about “network service provider”* (论“网络服务提供者”的法律界定), *Academic Exchange (学术交流)* Serial No. 267, No. 6, Jun, 2016, at 96.

1. The “Safe harbor” doctrine and the “notice and takedown” provision

The DMCA established a doctrine called “Safe Harbor”¹⁹ for ISPs. The purpose is to provide a balance between protecting copyright holders and ISPs’ liability. In order to be protected by safe harbor from direct or secondary liability, ISPs must follow the notice-and-takedown provision.²⁰ The notice-and-takedown provision requires copyright owners send a proper notification to ISPs when they find out infringing material on ISPs server. Upon receiving notification, ISPs must promptly remove or block access to the alleged material in order to obtain exemption from copyright liability. China adopted safe harbor doctrine in the RCI Regulation in 2006,²¹ and also enacted notice-and-takedown provision in Article 14 of the RCI Regulation. Japan also has a similar legal model in its Limitation of Provider Liability Act.

Most jurisdictions contain these two similar core principles: the safe harbor doctrine and the notice-and-takedown provision. These two traditional principles require ISPs to act passively on copyright protection until the copyright owners send notification regarding copyright infringement. The ISPs should react according to the notification in order to obtain protection from the safe harbor. In sum, a traditional passive-reactive ISP model requires ISPs to act passively and neutrally.²²

2. User Generated Content

Since copyright law provides ISPs a “Safe Harbor,” it is very hard to sue ISPs for direct infringement because most of the content are provided by its end-user, which is called User Generated Content (UGC). Most of the UGC services in China are free, and the ISPs

¹⁹ 17 U.S.C. § 512.

²⁰ 17 U.S.C. § 512(c)(1), See also 17 U.S.C. § 512 (d).

²¹ JERRY JIE HUA, TOWARD A MORE BALANCED APPROACH: RETHINKING AND READJUSTING COPYRIGHT SYSTEM IN THE DIGITAL NETWORK ERA, 102 (Springer 2014).

²² JEREMY & CHRISTOPHER, *supra* note 2, at 377.

derive their primary revenue from the number of times their advertisements are viewed.²³ Therefore, ISPs are usually held secondarily liable for copyright infringement. Based on the “Safe Harbor” doctrine, different countries have slightly different secondary liability theories. Nevertheless, copyright infringement cases about ISPs in the U.S., China, and other jurisdictions show that courts will generally consider several factors in order to determine whether the ISP will undertake the liability: first, whether the ISP knows if there are infringing activities by its end-user; second, whether the ISP is able to control the access or infringing activities; third, whether the ISP intends for the infringing activities to occur; and fourth, whether the ISP acquires direct financial benefits through infringing activities.²⁴

3. Legal Issues in China

In China, ISP legal system is criticized for being ineffective and inflexible. For example, a copyright owner may send a notification to Baidu because the owner finds infringing material on Baidu’s website. Following the notice-and-takedown provision, Baidu removed the material immediately and blocked the uploader’s account. However, after a few days, the copyright owner may find out that the material appears again on Baidu’ website because the Internet users can easily create multiple user accounts and upload digital files. A similar situation may happen again and again, and Baidu can always use the safe harbor doctrine to gain exemption from copyright liability. Some copyright owners in China believe that Baidu “abused” the safe harbor doctrine and asked for legal reform. Also, although Baidu kept losing copyright infringement cases for years, the situation has never been changed and copyright holders can hardly do anything to stop Baidu from copyright infringing activities.

²³ SEAGULL HAIYAN SONG, *NEW CHALLENGES OF CHINESE COPYRIGHT LAW IN THE DIGITAL AGE*, 25 (Wolters Kluwer 2011).

²⁴ *Id.* at 2.

The issue is that the legal model in these three jurisdictions requires the ISPs to behave passively until the copyright owners send the notification.²⁵ Such a legal model did not work well in China because ISPs usually take passive attitudes towards copyright protection as long as their own business are still working. However, according to some recent cases in these three countries, the courts has started to interpret ISP-related provisions from a passive-reactive approach to an active-preventive approach.²⁶ In *Viacom v. Google/YouTube*,²⁷ the Second Circuit decided that the DMCA Section 512(c)(1)(B) “requires something more than the ability to remove or block access to materials posted on a service provider’s website.”²⁸ Case and statutes in China also show that the court tends to require ISPs to play an active-preventive role instead of a passive-reactive role in copyright protection. This thesis will analyze ISP-related provisions and cases from the U.S., China and Japan in detail. Consequently, this thesis will suggest that the Chinese legislature should reform the ISP protection from a passive-reactive model to an active-preventive model for the purpose of better copyright protection.

²⁵ JEREMY & CHRISTOPHER, *supra* note 2, at 375.

²⁶ *Id.*

²⁷ *Viacom Int’l, Inc. v. YouTube, Inc.*, 718 F. Supp. 2d 514, 519 (S.D.N.Y. 2010).

²⁸ *Viacom*, 676 F.3d at 38. See also *Capitol Records, Inc. v. MP3tunes, LLC*, 821 F. Supp.2d 627, 646 (S.D.N.Y. 2011).

Chapter III

Approach to ISPs' Copyright Liability in the U.S.

In the digital era, the U.S. occupies the leading position of technological innovation. As new copyright issues arise along with new technology, the courts in the U.S. set several precedents for the new copyright issues and developed complete copyright infringement theories. These precedents and legal theories influence other jurisdictions, including China and Japan. This chapter examines the copyright liability theories of ISPs through three different ways: the DMCA statutes, the precedents of ISP and two recent ISP cases in the U.S.

ISPs can easily involve copyright infringement for the infringing material on their network. In *Aereo*, the U.S. Supreme Court held that Aereo infringes the public performance right of the broadcast company by its retransmitting service.²⁹ The Supreme Court decision may influence the legality of other technology, such as Cloud. The decision also exposes uncertainty of secondary transmission rights for online retransmit providers, which in turn may cause a chilling effect on ISPs and technological innovation. As a result, ISPs may lose incentives to provide online service that contains controversial technology.

In *YouTube*, in determining whether an ISP has actual knowledge about the infringing material on its network, the Second Circuit formulated a “subjective and objective standard” to solve the issue and suggested a “something more” standard that requires ISP to take more active steps to prevent copyright infringement.³⁰ Chinese and Japanese Court also applied the similar standard to determine whether an ISP “should have known” about the infringing

²⁹ *Aereo*, 134 S. Ct. at 2506.

³⁰ *Viacom*, 676 F.3d at 38.

material. In *Baidu*, the Beijing High People’s court required that the ISP should pay “reasonable duty of care”³¹ on copyright infringement, which is a similar requirement as something more standard. Chapter IV introduces the subjective and objective standards in China and Japan and Chapter V compares the difference among them.

A. Historical Context of ISP’s Copyright Liability

This section introduces the safe harbor doctrine of the DMCA and the development of the ISPs’ third party liability theories.

1. Background

With the development of network technology, anyone who has access to the Internet can easily make multiple perfect copies of an original work and distribute the digital copy of the work by uploading them onto a server; for example, by sending an attachment to others by email or uploading a file to Cloud. Normal users can easily find these digital works by the strong searching and linking capabilities of network technology.³² Due to the huge amount of network users, normal users may easily infringe copyright work as long as their activities are not authorized by copyright owners.

These direct infringers are difficult to locate due to the anonymity of the Internet. Moreover, skilled digital technology users can easily revise, modify, and adapt copyright works by using different technological tools. It is almost impossible for copyright owner to confirm and sue all the direct infringers. For example, it is very hard to locate a network user

³¹ Běijīng zhōng qīng wén wénhuà chuánméi yǒuxiàn gōngsī děng zhùzuòquán quán shǔ, qīnquán jiūfēn èrshěn mínshì pàn jué shū (北京中青文文化传媒有限公司等著作权权属、侵权纠纷二审民事判决书) [*China Youth Publishing Group v. Baidu Wenku*], 2014 Gao Min Zhong Zi No. 2045 (Beijing High People’s Ct. Aug 5, 2014), at 7.

³² HUA, *supra* note 21, at 101.

if the user is using a virtual private network (VPN), because VPN can show a different IP address instead of the real the IP address of the user. As a result, copyright owners tend to make actions against intermediaries, such as ISPs, who provide the platform to all the users. Although the ISPs seldom copy or distribute copyright works directly, the technologies and devices they provide may facilitate the direct infringers and therefore they may be responsible for secondary liabilities.

2. Direct Infringement

In the digital world, anyone who knows how to use electronics can easily make copies of the original copy work. Therefore, in traditional copyright doctrine, a third party who copies the original work without the author's authorization is considered as direct infringement. In order to sustain an action for direct infringement, the copyright owner must prove three things: first, the ownership of a valid copyright for the work. Second, the copyright owner has to prove that the work was copied by the defendant. Third, the owner must prove that the defendant's copying constitutes an improper appropriation.³³ Normally, an ISP who is facing a direct infringement lawsuit may claim safe harbor protection, and the copyright owner can claim secondary liability.

3. Secondary Liability

If ISPs provide copyright work on their server to the public without authorization by copyright owners, they can be liable for direct infringement. Most often, ISPs do not provide copyright content by themselves. It is their users who upload the infringing copyright work to their servers. Therefore, ISPs are usually held as secondary liability because their services facilitate the direct infringement of their users. Although the secondary liability may be harsh

³³ MARSHALL A. LEAFFER, UNDERSTANDING COPYRIGHT LAW 419 (LexisNexis 5th ed. 2010).

since the ISPs may have no actual knowledge of what their users did, one can be held liable for actively aiding another to infringe copyright.³⁴ While the Copyright Act does not expressly impose liability on anyone other than direct infringers, courts have recognized that vicarious or contributory liability will be imposed in certain circumstances.³⁵

4. Contributory Liability

The contributory infringement doctrine originated in tort law and stemmed from the principle that one who directly contributes to another's infringement should be accountable. In other words, the common law doctrine that one who knowingly participates in or furthers a tortious act is jointly and severally liable with the principal tortfeasor and is applicable under copyright law.³⁶ In order to establish a contributory liability claim, a copyright owner must prove that: (1) there is a direct infringement by a primary infringer; (2) the ISP has actual or constructive knowledge of the infringing activity; (3) the ISP should have caused or materially contributed to the underlying direct infringement.³⁷

5. Vicarious Liability

Unlike contributory infringement, under vicarious liability theory, even though the defendants are not aware of the infringing activity, they can be held liable due to the direct infringement of a third party. In order to establish a vicarious liability claim, a copyright owner needs to prove that: (1) there should be a direct infringement by a primary infringer; (2) the ISP has the right and ability to control or supervise the underlying direct infringement; (3)

³⁴ LEAFFER, *supra* note 32, at 438.

³⁵ *See Sony Corp. of America v. Universal City Studios, Inc.*, 464 U.S. 417, 435, 104 S. Ct. 774, 785, 78 L.Ed.2d 574 (1984).

³⁶ *Fonovisa, Inc. v. Cherry Auction, Inc.*, 76 F.3d 259, 264 (9th Cir. 1996).

³⁷ *Parker v. Google, Inc.*, 242 Fed.Appx. 833, 837 (3d Cir.2007).

the ISP derived a direct financial benefit from the underlying direct infringement.³⁸

B. Section 512 of the DMCA and Safe Harbor

1. The Online Copyright Infringement Liability Limitation Act (OCILLA)

It is possible that ISPs could be held contributory or vicarious liability for their users' infringing activities unknown to the ISPs. In order to limit ISPs' liability from copyright infringement, OCILLA was passed as a part of DMCA in 1998. The Act creates safe harbors for specified ISP activities: (1) transitory digital network communication; (2) system caching; (3) information residing on system or network at direction of users; (4) information location tools.³⁹ When ISPs' activities qualify in one of the categories, they are exempted from copyright liability.

In order to trigger any of the exemptions from safe harbor provisions, an ISP must meet two threshold conditions from Section 512(i): (1) a service provider must adopt, implement, and inform its users of its policy that provides termination of users who are repeat infringers.⁴⁰ (2) The ISP must accommodate and not interfere with standard technical measures that are used by copyright owners to identify and protect copyrighted works.⁴¹

2. Section 512(c)-(d)

In addition to the general provisions from Section 512(i), recent UGC liability cases are related to Section 512(c) and (d). These two statutes might immunize the ISP that unintentionally host infringing content uploaded by its users. In addition to the two general threshold requirements with which ISPs must comply, Section 512(c) also requires the ISP

³⁸ Gershwin Publishing Corp. v. Columbia Artists Management, Inc., 443 F.2d 1159, 1162 (2d Cir.1971).

³⁹ 17 U.S.C. § 512(a)-(d).

⁴⁰ 17 U.S.C. § 512(i)(1)(A).

⁴¹ 17 U.S.C. § 512(i)(1)(B).

that: (1) does not have actual knowledge or is aware of facts or circumstances from which infringing activity is apparent;⁴² (2) does not receive financial benefits directly attributable to the infringing activity, in a case in which the service provider has the right and ability to control such activity,⁴³ and (3) acts expeditiously to remove or disable access to the purported infringing material, upon obtaining such knowledge or awareness or receiving notice from copyright owners or their agents.⁴⁴

C. ISP's Copyright Liability established by Common Law Cases

1. Sony Safe harbor rule

Before the DMCA was enacted in 1998, *Sony Corp. v. Universal City Studios Inc.*⁴⁵ was an influential case that established safe harbor system for technological intermediaries. The issue was whether Sony's new product, Betamax video cassette recorder (VRC), which could be used both for legal time-shifting purpose and unlawful purpose of copyright infringement, indirectly infringed Universal's copyright. The U.S. Supreme Court borrowed a staple article of commerce doctrine from the U.S. Patent Law⁴⁶ and concluded that "the sale of a 'staple article or commodity of commerce suitable for substantial noninfringing use' is not contributory infringement." The court held that the VRC was capable of substantial noninfringing use and therefore could not be banned.

⁴² 17 U.S.C. § 512(c)(1) & § 512(d)(1).

⁴³ 17 U.S.C. § 512(c)(2) & § 512(d)(2).

⁴⁴ 17 U.S.C. § 512(c)(3) & § 512(d)(3).

⁴⁵ *Sony Corporation of America v. Universal City Studios Inc.*, 104 S. Ct. 774 (1984).

⁴⁶ See 35 U.S.C. § 271(c).

2. Inducement theory

In *MGM v. Grokster* case,⁴⁷ the U.S. Supreme Court analyzed the holding in *Sony* and staple article of commerce doctrine from patent law, and concluded that the Court of Appeals misunderstood Sony rule because “Sony’s staple-article rule will not preclude liability.”⁴⁸ After citing several case of inducement infringement, the Supreme Court adopted the inducement rule from Patent Law and held that “one who distributes a device with the object of promoting its use to infringe copyright, as shown by clear expression or other affirmative steps taken to foster infringement, is liable for the resulting acts of infringement by third parties.”⁴⁹

As a conclusion of inducement theory, to prove an ISP’s secondary liability for copyright infringement, a copyright owner has to show: (1) the ISP has actual knowledge of infringing conduct; (2) the ISP had an affirmative intent or step to incite direct copyright infringement.

D. Cases

This section introduces and analyzes two recent cases in the U.S. The *Aereo* case addresses a new ISP issue about public performance right. The U.S. Supreme Court held that *Aereo*’s new technology and device infringes the public performance right, but the case decision did not provide a complete solution to solve similar issues in other network technology. While this issue happened in *Baidu* and *Winny* cases, courts in China and Japan provided their own approach to this issue.

In the *YouTube* case, the Second Circuit discussed Section 512(c)(1)(A)(ii) of the DMCA, the so called “Red Flag” knowledge provision and suggested two rules: the

⁴⁷ *Metro-Goldwyn-Mayer Studios Inc. v. Grokster Ltd.*, 125 S. Ct. 2764 (2005).

⁴⁸ *Grokster*, 125 S. Ct., at 2779.

⁴⁹ *Id.* at 2780.

subjective and objective standard, and the “something more” doctrine. In the *Baidu* case, the Beijing High People’s Court also adopted similar theories. In the *Winny* case, Justice Otani suggested these theories while the majority took a different approach.

Chapter IV examines details from the *Baidu* and *Winny* cases and Chapter V compares these cases from three countries to propose a solution for the issue of secondary liabilities.

1. *American Broadcasting Cos. v. Aereo, Inc.*

a. Background

*ABC v. Aereo*⁵⁰ is one of the most recent cases involving ISPs from the U.S. Supreme Court. Generally speaking, Aereo captures and transcodes over-the-air broadcast television programming signals by its miniature antenna per every customer, and then retransmits the programming from its server through the Internet to its subscribers. “Aereo neither owns the copyright in those works nor holds a license from the copyright owners to perform those works publicly.”⁵¹ Different from other ISP copyright infringement cases, the plaintiffs focused their claim on direct infringement of public performance right.⁵² Although transmitting or retransmitting a copyrighted work without the authorization of a copyright owner is considered a copyright infringement, the definition of secondary transmission of ISPs under Copyright Act is unclear. Therefore, how to determine an ISP’s secondary liability for performance and reproduction infringement is a question.

b. Secondary ISP liabilities

In the dissent of court’s decision by Scalia, J, the court first goes through case law about

⁵⁰ *Am. Broad. Companies, Inc. v. Aereo, Inc.*, 134 S. Ct. 2498 (2014).

⁵¹ *Id.* at 2503.

⁵² 17 U.S.C. § 106(4).

direct and secondary liability for copyright infringement:

...[Direct infringement] applies when an actor personally engages in infringing conduct. See *Sony Corp. of America v. Universal City Studios, Inc.*, 464 U.S. 417, 433, 104 S.Ct. 774, 78 L.Ed.2d 574 (1984). Secondary liability, by contrast, is a means of holding defendants responsible for infringement by third parties, even when the defendants “have not themselves engaged in the infringing activity.” *Id.*, at 435, 104 S.Ct. 774. It applies when a defendant “intentionally induc[es] or encourag[es]” infringing acts by others or profits from such acts “while declining to exercise a right to stop or limit [them].” *Metro-Goldwyn-Mayer Studios Inc. v. Grokster, Ltd.*, 545 U.S. 913, 930, 125 S.Ct. 2764, 162 L.Ed.2d 781 (2005).

Most suits against equipment manufacturers and service providers involve secondary-liability claims...⁵³

For ISP’s direct liability, a volitional conduct rule should be applied, which requires that the defendant’s conduct be directed to the plaintiff’s copyrighted material. Moreover, “The defendant may be held directly liable only if the defendant himself ‘trespassed on the exclusive domain of the copyright owner.’”⁵⁴ Nevertheless, the fundamental difference of this case is whether Aereo operated an automated, user-controlled system and infringed plaintiffs’ public performance right.⁵⁵

c. Public Performance Right

In the Copyright Act, “To perform a work ‘publicly’ means [among other things] to transmit ... a performance ... of the work to the public.”⁵⁶ Undoubtedly, Aereo does not have any exclusive right to transmit any copyright works. It merely provides an online service to retransmit broadcast signal over the Internet to its subscribers. In opinion of SCALIA, J, he argued that Aereo’s retransmission service is just like “a copy shop that provides its patrons with a library”⁵⁷ and since “the producer of a technology

⁵³ *Id.* at 2512 (Scalia, J., dissenting).

⁵⁴ *Id.* Citing *CoStar Group, Inc. v. LoopNet, Inc.*, 373 F.3d 544, 550 (4th Cir.2004).

⁵⁵ 17 U.S.C. § 106(4).

⁵⁶ 17 U.S.C. § 101.

⁵⁷ *Aereo.*, 134 S. Ct. at 2514 (Scalia, J., dissenting).

which permits unlawful copying does not himself engage in unlawful copying,”⁵⁸ Aereo does not “perform” and shall not be held directly liable for infringing plaintiffs’ public-performance right. On the contrary, the majority considers Aereo as a community antenna television (CATV) company. The court believed that “this solo technological difference between Aereo and traditional cable companies does not make a critical difference here” and concluded “Aereo is not just an equipment supplier and that Aereo ‘perfrom[s]’.”⁵⁹

d. Secondary transmission right

Since the majority considered “Aereo’s activities are substantially similar to those of the CATV companies...”⁶⁰, Copyright Act Section 111 which governs cable television system may be helpful for analyzing secondary transmission of ISP. According to Section 111(f)(1)-(2), “a ‘primary transmission’ is a transmission made to the public by a transmitting facility whose signals are being received and further transmitted by a secondary transmission service...”⁶¹ and “a ‘secondary transmission’ is the further transmitting of a primary transmission simultaneously... or nonsimultaneously with the primary transmission...”⁶² The question is whether an ISP’s secondary transmission of a primary transmission be considered a public performance. In this case, the court held that “Aereo transmits a performance of petitioners copyrighted works to the public, within the meaning of the Transmit Clause.”⁶³ Is this ruling able to apply to all other online retransmit services, such as Peer-to-Peer Assisted Streaming Television (P2PTV)? In a P2PTV system, each user, while downloading a video stream, is simultaneously also uploading that stream to other users, which makes all the users as a “secondary transmitter” and therefore performing copyrighted

⁵⁸ *Grokster*, 545 U.S., at 960, 125 S. Ct. 2764 (Breyer, J., concurring)

⁵⁹ *Aereo*, 134 S. Ct. at 2507.

⁶⁰ *Aereo*, 134 S. Ct. at 2506.

⁶¹ 17 U.S.C. § 101(f)(1).

⁶² 17 U.S.C. § 101(f)(2).

⁶³ *Aereo*, 134 S. Ct. at 2510.

work to the public under this rationale.

The problem of this rationale is that the court considered Aereo as CATV, but did not apply CATV regulations to this case because the ISPs are not regulated by the Federal Communications Commission (FCC).⁶⁴ From a technical perspective, Aereo's cloud system is almost the same as Remote Storage Digital Video Recorder system ("RS-DVR") provided by CATV companies, which allows their customers to make copies of television programming, to store them on their hard drives, and to enjoy extra functions, such as playback for later viewing. The Court of Appeal believed in this view and cited a holding from *Cartoon Network LP, LLLP v. CSC Holdings, Inc.*, a case about RS-DVR issue of CATV.⁶⁵ The Supreme Court cited its holding from the Court of Appeal that "Aereo does not perform publicly within the meaning of the Transmit Clause because it does not transmit 'to the public.' Rather, each time Aereo streams a program to a subscriber, it sends a private transmission that is available only to that subscriber."⁶⁶ If Aereo's system provides the same playback service like RS-DVR, and the court considered Aereo as CATV company, then why did the Supreme Court make the opposite decision on Aereo?

One reason might be that although Aereo provided almost the same RS-DVR service to its subscriber, unlike the CATV company, Aereo paid no royalties to copyright owners. Under Copyright Law, an authorized retransmitter has to pay royalties to copyright owners. For example, under the statutory license for CATV systems,⁶⁷ a CATV company needs to obtain a license from an over-the-air broadcast company in order to retransmit its signal through their CATV network. If the court decides that Aereo's transmission is a private performance, therefore *Aereo* does not need to obtain a license from copyright owners, and it is unfair for current CATV company to continue their business.

⁶⁴ 17 U.S.C. § 106(f)(3).

⁶⁵ See *WNET, Thirteen v. Aereo, Inc.*, 712 F.3d 676 (2013).

⁶⁶ *Aereo*, 134 S. Ct. at 2504.

⁶⁷ 17 U.S.C. § 111.

e. Impacts on Cloud technology

The court noticed the influence of the holding of this case and supplied that “it does not determine whether different kinds of providers in different contexts also ‘perform’” and “it does not extend to those who act as owners or possessors of the relevant product.”⁶⁸ The court has “not considered whether the public performance right is infringed when the user of a service pays primarily for something other than the transmission of copyrighted works, such as the remote storage of content.”⁶⁹ However, if a user uploads a movie to “Cloud storage,” such as “Baidu Cloud,”⁷⁰ in order to watch it online at a later time, is “Baidu Cloud” also involved in “secondary transmission”? Furthermore, “Baidu Cloud” allows its users to share any materials in their accounts to the other users. For example, if a user finds a movie shared by the other user and watches it online, does “Baidu Cloud” also perform a copyrighted work to public?

The *Aereo* case does not answer these questions and we may seek the answers elsewhere. Aereo’s retransmission service is similar to the video-on-demand service like Netflix⁷¹ except one thing: Aereo neither owns the copyright nor is authorized by the copyright owner. Some of the broadcasts retransmitted by Aereo were in the public domain. Some were copyrighted, which might cause a secondary liability for performance and reproduction infringement. Although the Supreme Court didn’t provide a test to determine how to apply the Transmit Clause to new technology, we may conclude from the court’s decision that copyright owner’s authorization is essential. ISPs are not allowed to retransmit any copyrighted works for free without copyright owner’s authorization. If Aereo negotiated with

⁶⁸ *Aereo*, 134 S. Ct. at 2510.

⁶⁹ *Aereo*, 134 S. Ct. at 2511.

⁷⁰ A cloud storage service provide by “Baidu,” almost the same as “Dropbox” in the U.S.

⁷¹ *How does Netflix work?* NETFLIX, <https://help.netflix.com/en/node/412?lang=en&nodeId=412> (last visited Aug. 27, 2016).

over-the-air broadcast companies and purchased the licenses for the copyrighted works, just like CATV company under Section 111, the result might be different. However, in UGC services, the users share the content instead of ISPs. User may derive content legally, but may still obtain copyrighted work without the authorization of the copyright owner. In this case, the court reached the secondary liability analysis and believed that the Congress should make specific rules about the retransmission right of ISPs. ISPs' secondary liability has been discussed by different U.S. courts and the topics will focus on it in the next case below.

2. *Viacom v. Google/YouTube*

One of the most recent cases about ISP safe harbor doctrine is *Viacom v. Google/YouTube*.⁷² Viacom brought a lawsuit against YouTube and its parent company, Google, for direct and secondary copyright infringements on March 13, 2007. YouTube is one of the most popular UGC video-sharing websites that allows its users to watch, upload, and share personal clips on its website and watch the video free of charge.⁷³ To upload a video to YouTube, a user must register and create an account by email first. Secondly, the user must accept YouTube's Terms of Agreement which requires the user "not submit material that is copyrighted ... unless [he is] the owner of such rights or ha[s] permission from their rightful owner to post the material and to grant YouTube all of the license rights granted herein."⁷⁴ After the registration is completed, the user is able to upload any videos on their personal computers, mobile phones or other devices to YouTube's server. YouTube will make copies and transcode this original video format in order to stream the video on its website to the other users all over the world.

⁷² *Viacom Int'l, Inc. v. YouTube, Inc.*, 676 F.3d 19 (2d Cir. 2012).

⁷³ *Id.* at 28.

⁷⁴ *Id.*

a. Section 512(c)(1)

In order to provide online service, an ISP such as YouTube may use technological processes to make, transmit and download multiple copies of its user's stored materials. When someone wants to access its online material, the website will respond to the user's request and transmit relevant content from the server to the user's computer. According to Section 512(c)(1), an ISP is under protection of safe harbor if the infringing activity occurs "by reason of the storage at the direction of a user of material that resides on a system or network controlled or operated by or for the service provider."⁷⁵ For example in this case, YouTube is considered an ISP because it operates a service for users to store videos on its server, and YouTube therefore qualifies for safe harbor protection under Section 512(c)(1).

To provide "storage" service to its users, an ISP may provide multiple kinds of software so that the users can upload or gain access to their stored materials. These software works automatically by different computer algorithm to provide different services to Internet users. For example, just as people would like to put food into a container before storing it in the refrigerator, in order to store a user's material on its server, an ISP prefers to modify user-submitted material during the uploading process for multiple reasons, such as saving storage space, data maintenance, etc. As a result, besides storage service, an ISP may also provide other services based on its business. Therefore, the issue in Section 512(c)(1) is clear: how to interpret the word "storage"? Does it merely means storing material or including its relevant technological processes?

In this case, YouTube uses automated software function to (1) transcode the uploaded material to a different encoding scheme; (2) stream video to users and respond to playback request; (3) display links to users with related video.⁷⁶ The court of appeal agreed with the

⁷⁵ 17 U.S.C. § 512(c)(1).

⁷⁶ *Viacom*, 676 F.3d at 28.

District Court's decision that "...the word 'storage' is too narrow to meet the statute's purpose"⁷⁷ and held that these three software functions are protected by Section 512(c).⁷⁸ All these three software functions are closely related to the stored material on the ISP website and works automatically to facilitate access to ISP's service. In *UMG Recordings, Inc. v. Shelter Capital Partners LLC*, 718 F.3d 1006 (UMG), a recent case from the Ninth Circuit, the court agreed with this opinion and held that "the language and structure of the statute ... clarify that Section 512(c) encompasses the access-facilitating processes that automatically occur when a user upload a video to Veoh."⁷⁹ From these holdings, the courts tend to protect ISPs that provide storage service under Section 512(c)(1), as long as the service of the ISPs function to facilitate access to user-stored material.

The other issue of Section 512(c) contains the phrase "at the direction of a user." Although an ISP may request its user to sign Terms of Agreement of its service, it is the employee of an ISP who programs the algorithm and facilitates its online service. On the other hand, a user of ISP may not even know how these software functions work and the programmer of an ISP can easily change the functions without user's awareness or consent. To some extent, an ISP actually involved in its user's decision and encourages its user to do what they want by providing storage services. So far the court has not focused on this related issue on Section 512(c).

b. Actual knowledge provision Section 512(c)(1)(A)(i)⁸⁰ and "Red Flag" knowledge provision Section 512(c)(1)(A)(ii)⁸¹

⁷⁷ *Viacom*, 718 F. Supp. 2d at 526.

⁷⁸ *Viacom*, 676 F.3d at 39

⁷⁹ *UMG Recordings, Inc. v. Shelter Capital Partners LLC*, 718 F.3d 1006, 1016 (9th Cir. 2013).

⁸⁰ 17 U.S.C. § 512(c)(1)(A)(i): does not have actual knowledge that the material or an activity using the material on the system or network is infringing;

⁸¹ 17 U.S.C. § 512(c)(1)(A)(i): in the absence of such actual knowledge, is not aware of facts or circumstances from which infringing activity is apparent;

First of all, when determining whether an ISP qualifies for Section 512(c) safe harbor protection, the district court believes that the critical question is whether the statutory language of Section 512(c)(1)(A)(i) and (ii) mean a “general awareness that there are infringements” or rather mean “actual or constructive knowledge of specific and identifiable infringements of individual items.”⁸² The court of appeal agreed with the holding of the district court that the statutory phrases “actual knowledge that the material ... is infringing” and “facts or circumstances from which infringement activity is apparent” refer to “knowledge of specific and identifiable infringements.”⁸³ Furthermore, the court of appeal pointed out a subjective and objective standard between two provisions:

[T]he actual knowledge provision turns on whether the provider actually or “subjectively” knew of specific infringement, while the red flag provision turns on whether the provider was subjectively aware of facts that would have made the specific infringement “objectively” obvious to a reasonable person....both provisions do independent work, and both apply only to specific instances of infringement.⁸⁴

In other words, the subjective standard refers to actual knowledge of specific infringement, such as whether the ISP has received the notification from a copyright owner. On the other hand, the objective standard refers to whether the infringement fact is apparent enough to a reasonable person. For example, a popular Rio Olympic Games video that was uploaded by an anonymous Internet user instead of the official organization or entity is likely to be an infringing material to a reasonable person. This opinion was also accepted in the *UMG* case. The Ninth Circuit quoted the same paragraph above and pointed out that in determining whether the ISP was aware of a red flag, a subjective standard should be applied first. In deciding whether the subjective facts constitute a red flag, an objective standard should be used.⁸⁵

⁸² *Viacom Int'l, Inc. v. YouTube, Inc.*, 718 F. Supp. 2d 514, 519 (S.D.N.Y. 2010).

⁸³ *Id.* at 523.

⁸⁴ *Viacom*, 676 F.3d at 31.

⁸⁵ *UMG Recordings, Inc. v. Shelter Capital Partners LLC*, 718 F.3d 1006, 1026 (9th Cir. 2013).

Generally, an ISP may always know that its service may be used as infringing activity. But such vague knowledge does not qualify as the actual knowledge provision. Section 512(c)(1)(A)(i) requires specific and subjective facts about infringing activity. While red flag knowledge provision requires such knowledge would have been apparent to a reasonable person to be aware of the existence of specific infringing activity. Thus, the requirements for an ISP qualify a safe harbor protection under Section 512(c)(1)(A) is clear: (1) unaware of facts that indicate specific and identifiable instances of infringement; (2) expeditious removal after an ISP knows exactly which items to remove.

c. Section 512(c)(1)(B)

Even if an ISP qualifies for safe harbor protection under Section 512(c)(1)(A), Section 512(c)(1)(B) requires an ISP “has the right and ability to control” the infringing activity. The District Court believes that “an ISP must have specific knowledge of the infringing activity before he can control.”⁸⁶ While the Court of Appeal held that “§512(c)(1)(B) does not include a specific knowledge requirement” and “requires something more than the ability to remove or block access to materials posted on a service provider’s website,”⁸⁷ however, the Court didn’t discuss this so-called “something more” standard in depth. Consequently, the question is what an ISP should do in order to qualify for safe harbor protection under Section 512(c)(1)(B)?

The Court gives two examples about this something more standard, suggesting an ISP “exert substantial influence on the activities of users” such as “institute a monitoring program” or “forbid certain types of content and refuse access to users who failed to comply with its

⁸⁶ *Viacom*, 718 F. Supp. 2d at 527.

⁸⁷ *Viacom*, 676 F.3d at 38. See also *Capitol Records, Inc. v. MP3tunes, LLC*, 821 F. Supp.2d 627, 646 (S.D.N.Y. 2011).

instructions.”⁸⁸ The Ninth Circuit agreed with this opinion and held that “substantial influence” may include “high levels of control over activities of users” or “purposeful conduct.”⁸⁹ In *YouTube*, ISP’s antipiracy efforts may be considered exercising substantial influence on its users, such as the adoption of Audible Magic fingerprint filtering technology that will “remove an offending video automatically if it matched some portion of a reference video submitted by a copyright owner who had designated this service.”⁹⁰ As a conclusion from these cases, the something more standard requires an ISP to show their ability to prevent its users from uploading infringing copyrighted content, and control its repeated infringers by taking concrete action, such as terminating a repeated infringer’s account, etc. Moreover, the something more standard indicates that the court actually requires ISP to take active steps to prevent copyright infringement instead of hiding behind safe harbor protection. The next chapter introduces the reasonable duty of care requirement in China, which has a similar rationale to the something more standard. Chapter V compares these two ISP approaches and demonstrates that the new trend of ISP model is shifting from a passive-reactive ISP model to an active-preventive model.

⁸⁸ *Id.* See also *Perfect 10, Inc. v. Cybernet Ventures, Inc.*, 213 F.Supp.2d 1146 (C.D.Cal.2002).

⁸⁹ *UMG Recordings, Inc. v. Shelter Capital Partners LLC*, 718 F.3d 1006, 1030 (9th Cir. 2013).

⁹⁰ *Viacom*, 718 F. Supp. 2d at 528.

Chapter IV

Chinese and Japanese Approach to ISP's Copyright Liability

This Chapter introduces background information about Chinese and Japanese ISP policy, and examines recent ISP cases from China and Japan. For the purpose of deep discussion in chapter V, this chapter also analyzes similarities and difference among ISP policies in China, Japan and the U.S.

Baidu is a technology company in China that provides multiple online services, including search engine, Cloud, etc. After Google left Chinese search engine market in 2010,⁹¹ Baidu occupied most of the Chinese search engine market. In the Search Advertisement Spending market worldwide, Baidu is next-largest company than Google, with 8.8% share of the \$81.59 billion market.⁹² To some extent, copyright infringement issues on Baidu reflect the copyright protection flaws in China. From 2010 to 2014, Baidu was involved in multiple copyright infringement lawsuits against copyright owners. This Chapter focuses on the Baidu Wenku case as a typical ISP case.

In Japan, the legislature has amended its Copyright Law in 2009 to adopt a new technology environment. This Chapter examines Japanese ISP policy by *Winny*, the first P2P software case from the Japanese Supreme Court. The fact in *Winny* case is similar to the fact in *Grokster* case in the U.S. However, the Japanese Supreme Court issued an opposite decision than the one issued in *Grokster*. This judicial decision shows that Japan still follows

⁹¹ Miguel Helft & Michael Wines, *Google Faces Fallout as China Reacts to Site Shift* (Mar. 23, 2010), http://www.nytimes.com/2010/03/24/technology/24google.html?pagewanted=1&_r=0&hp (last visited Oct 7, 2016).

⁹² *Google Will Take 55% of Search Ad Dollars Globally in 2015*, EMARKER, <http://www.emarketer.com/Article/Google-Will-Take-55-of-Search-Ad-Dollars-Globally-2015/1012294> (last visited Nov. 3, 2016).

a traditional passive-reactive ISP trend, while the trend in China and the U.S. is an active-preventive approach for ISP. Comparative analysis of these three countries' approach is discussed in Chapter V.

A. China's New Approach to ISPs' Copyright Liability

1. New Developments in ISP Copyright Liability in China

According to the 37th Statistical Report on Internet Development in China (Jan 2016)⁹³ from China Internet Network Information Center (CNNIC), “until December 2015, the number of Chinese Internet users was about 668 million and the penetration rate reached 50.3%, up 2.4 percentage points from the end of 2014.” With a remarkable increase of mobile Internet users (90.1% of the total netizen population, 85.8% in 2014), it is much more convenient for Internet users to reach entertainment and enjoyment copyright contents on Internet. 73.2% of Internet users were subscribers of online video, and the number of subscribers of online music reached 501 million. ISP issues remain a bottleneck issue to the development of online copyright industry. For example, “the National Copyright Administration issued the Circular on Demanding Online Music Providers to stop marketing Unauthorized Music Works on July 8, 2015, and launched a campaign to regulate the copyright issue of online music.”⁹⁴ Therefore, establishing certainty about the liability for ISPs in order to balance the interest between copyright owners and Internet users remain an important task.

⁹³ CNNIC, 37th Statistical Report on Internet Development in China, at 1. http://cnnic.cn/hlwfzyj/hlwzxbg/hlwjbg/201601/t20160122_53271.htm (last visited Sep 8th, 2016). English version is available at <http://cnnic.com.cn/IDR/ReportDownloads/>.

⁹⁴ *Id.* at 82.

2. Statutory Development

a. Amended Copyright Law of the PRC

With the development of network technology and the wave of digitization (digitize information), Chinese legislature noticed that the 1990 RPC Copyright Law was no longer suitable for the new legal environment in information age. Therefore, it was later revised twice. RPC Copyright Law was revised for the first time in 2001 in order to qualify the minimum protection standard of TRIPS Agreement.⁹⁵ The second revision was made in 2010 to fulfill the ruling of WTO about IP issue between China and the U.S.⁹⁶ However, the RPC Copyright Law provides limited protection to copyright owners in the digital world because it only defines some broad concepts and basic rights about copyright. One of the most important rights for copyright owners is “the right to communicate works to the public over information networks” (right of dissemination through information network): “The term ‘copyright’ shall include the following personality rights and property rights...that is, the right to communicate to the public a work, by wire or wireless means in such a way that members of the public may access these works from a place and at a time individually chosen by them.”⁹⁷ However, there is no further interpretation about RCI in the amended 2010 PRC Copyright Law. Chinese legislature has already noticed this question and a third revision of Copyright Law is in progress. Legislative Affairs Office of the State Council PRC has already published a Copyright Law revision draft on January 6, 2014. So far the specific ISP-related provisions exist in the other PRC laws and regulations.

⁹⁵ Agreement on Trade-Related Aspects of Intellectual Property.

⁹⁶ Ji Chendi (姬晨笛), *Research on the Legal Nature of China's "Safe Haven" Rule* (我国“避风港”规则的法律性质研究), *Electronics Intellectual Property* (电子知识产权), Z1-2016, at 65.

⁹⁷ Zhong hua ren min gong he guo zhu zuo quan fa (中华人民共和国著作权法) [Copyright Law of the PRC] (promulgated by the Standing Comm. Nat'l People's Cong., Sep. 7, 1990, second amended by the Standing Comm. Nat'l People's Cong., Feb. 26, 2010), art. 10. The English translation is available at <http://www.cpahkltd.com/EN/info.aspx?n=20100429164418197504>.

b. Measures for the Administrative Protection of Internet Copyright Measures (ICM)

ICM is considered as the first administrative regulation about Internet copyright protection in China. It was promulgated by the National Copyright Administration (NCA) and the Ministry of Information Industry (MII) on April 30, 2005. ICM also adopted the “safe harbor” model from the U.S. DMCA, such as “take-down notice.” For example, Article 5 of ICM stipulates “Where a copyright owner finds any content communicated through Internet infringes upon its copyright, and sends a notice to the ISP... the ISP shall immediately take measures to remove the relevant content, and keep the copyright owner’s notice for 6 months.”

⁹⁸ Since ICM has so much overlap with a specific ISP law, which was promulgated one year after ICM, detail of this new ISP law will be discussed in next paragraph.

3. RCI Regulation

The specific regulations about ISP can be found in RCI Regulation, which was promulgated in 2006 and revised in 2013. Chinese legislature has followed the U.S. DMCA’s “safe harbor” model to regulate ISP liability and limitation. For example, similar to Section 512 of the DMCA, there are also four categories of ISP conducts under liability exemptions subject to certain conditions.

First, like Section 512(a) transitory digital network communication, Article 20 of RCI Regulation protects “An ISP that provides network automatic access service at the direction of its subscribers, or provides service for automatic transmission of works, performances, sound recordings or video recordings provided by its subscribers” as long as (1)“ the ISP neither chooses nor alters the transmitted works...” and (2)“ makes works ... available to the

⁹⁸ Hu lian wang zhu zuo quan xing zheng bao hu ban fa (互联网著作权行政保护办法) [Measures for the Administrative Protection of Internet Copyright Measures] (promulgated by NCA & MII, Apr. 29, 2005, effective May 1, 2005), art 5, translated by Bei da fa bao (en.pkulaw.cn).

designated recipients” rather than others.⁹⁹

Second, like Section 512(b) system caching, Article 21 of RCI Regulation protects “An ISP that provide the service of automatic storage for works, performances, sound recordings or video recordings obtained from another ISP in order to improve the efficiency of the network transmission, and provides them to its subscribers ...” as long as (1) “it does not alter the automatically stored works...” and (2) such storage does not affect the access of the initial ISP...”¹⁰⁰

Third, like Section 512(c) information residing on system or network at direction of users, Article 22 of RCI Regulation provides five prerequisites for an ISP “not be liable for compensation.”¹⁰¹ Article 22 paragraph 3 of RCI Regulation provides almost the same red flag provision in Section 512(c)(1)(A)(ii). In other words, Chinese safe harbor model also adopt the red flag test.¹⁰² In sum, Article 22 require: (1) the ISP does not know or have justifiable reasons to know about the infringing activities of the subscribers; (2) the ISP does not obtain any economic benefits from the infringing activity; (3) the ISP removes the works in question upon receiving notice from the copyright owners. Besides the requirement to

⁹⁹ Xin xi wang luo chuan bo quan bao hu tiao li (信息网络传播权保护条例) [Regulations for the Protection of the Right of Communication through Information Network] (promulgated by the St. Council, May 18, 2016, amended by the St. Council in Jan 30, 2013) art. 20. The English translation is available at <http://www.cpahkltd.com/UploadFiles/20100315165559735.pdf>.

¹⁰⁰ Regulations for the Protection of the Right of Communication through Information Network, art. 21.

¹⁰¹ Regulations for the Protection of the Right of Communication through Information Network, art. 22: Under the following circumstances, a network service provider that provides information storage space to a service object or provides works, performances, or audio-visual recordings to the public through the information network, shall not be liable for compensation:

1. Having clearly mentioned that the information storage space is provided to the service object, and also having publicized the name, contact information, and web address of the network service provider;
2. Having not altered the work, performance, or audio-visual recording provided to the service object;
3. Having not known and having no justified reason to know that the works, performances, or audio-visual recordings provided by the service object have infringed upon an other's right;
4. Having not directly obtained economic benefits from the service object's provision of the work, performance, or audio-visual recording;
5. After receiving the notification from the owner, having deleted the work, performance, or audio-visual regarded as infringing on the right of the owner according to the Provision of this Regulation.

¹⁰² Jiang Bo (江波) & Zhang Jinping (张金平), *Research on the ISP's knowledge standard – rethink “red flag provision”* (网络服务提供商的知道标准判断问题研究——重新认识“红旗标准”), *Journal of law application (法律适用)*, No. 12, 2009, at 55.

expeditiously remove the alleged infringing material, other factors are a combination of vicarious and contributory liability established in America law cases.¹⁰³

Fourth, like Section 512(d) information location tools, Article 23 of RCI Regulation protects “An ISP that provides searching or linking service to its subscribers,” as long as “it disconnects the link to the infringing works, performances, sound recordings or video recordings upon receipt of the right owner’s notification...” But, “it shall be jointly liable for the infringement if it knows or has reasonable grounds to know that the works...provided by its subscribers infringe another persons’ rights.”¹⁰⁴ Although the expression of RCI Regulation Art 20-23 are not exactly the same as the DMCA Section 512(a)-(d), the four categories of ISP conducts between two countries has almost the same function. However, the liability theory of RCI Regulation Article 23 is different from the DMCA, and the detail of this difference will be discussed in Chapter IV.

4. Tort Law of the PRC

The legal basis of “joint-liability”¹⁰⁵ theory can be found in Chinese Civil Code, which was enacted in 1987 The General Principles of the Civil Law of the PRC.¹⁰⁶ The PRC Tort Law, which was promulgated in 2010, applied this theory on ISP’s liability of direct infringement by its end-users. The principle of “joint-liability” can be found in PRC Tort Law Article 9: “One who abets or assists another person in committing a tort shall be liable jointly and severally with the tortfeasor . . .”¹⁰⁷ And the specific liability on ISP was enacted in Article 36, which can be divided into two parts: direct infringement and secondary

¹⁰³ HUA, *supra* note 2, at 111.

¹⁰⁴ Regulations for the Protection of the Right of Communication through Information Network, art. 23.

¹⁰⁵ Civ. Code of PRC, art. 130: If two or more persons jointly infringe upon another person’s rights and cause damage, they shall bear joint liability.

¹⁰⁶ The General Principles of the Civil Law of the PRC, art. 130.

¹⁰⁷ Zhong hua ren min gong he guo qing quan ze ren fa (中华人民共和国侵权责任法) [Tort Law of the PRC] (promulgated by the Standing Comm. Nat’l People’s Cong., Dec. 26, 2009, effective in Jul. 1, 2010) art. 9. The English translation is available at http://www.wipo.int/wipolex/en/text.jsp?file_id=182630.

infringement.

The first paragraph of Article 36 stipulates the direct infringement liability of ISP.¹⁰⁸ Like the DMCA§512(c)(1)(C), the second paragraph of Article 36 stipulates: “Where a network user commits a tort through the network services, the victim of the tort shall be entitled to notify the network service provider to take such necessary measures as deletion, block or disconnection. If, after being notified, the network service provider fails to take necessary measures in a timely manner, it shall be jointly and severally liable for any additional harm with the network user.” And, like DMCA§512(c)(1)(A), the third paragraph of Article 36 stipulates: “Where a network service provider knows that a network user is infringing upon a civil right or interest of another person through its network services, and fails to take necessary measures, it shall be jointly and severally liable for any additional harm with the network user.”¹⁰⁹ Although China applies the “joint-liability” theory on ISP instead of contributory or vicarious theories in the U.S., from the expression of PRC tort Law Article 36, Chinese court may consider similar factors on secondary liability of ISP. Chapter V provides a detailed discussion of these factors.

5. Provisions of the Supreme People's Court on Several Issues concerning the Application of Law in Hearing Civil Dispute Cases Involving Infringement of the Right of Dissemination on Information Networks¹¹⁰ (the Provision)

In China, the Supreme People’s Court is able to provide a so-called “judicial

¹⁰⁸ The PRC Tort Law, art. 36 para. 1: A network user or network service provider who infringes upon the civil right or interest of another person through network shall assume the tort liability.

¹⁰⁹ The PRC Tort Law, art. 36.

¹¹⁰ *Zui gao ren min fa yuan guan yu sheng li qing hai xin xi wang luo chuan bo quan min shi jiu fen an jian shi yong fa lv ruo gan wen ti de gui ding*(最高人民法院关于审理侵害信息网络传播权民事纠纷案件适用法律若干问题的规定) [Provisions of the Supreme People's Court on Several Issues concerning the Application of Law in Hearing Civil Dispute Cases Involving Infringement of the Right of Dissemination on Information Networks] [hereinafter “the Provision”](promulgated by the Sup. People’s Ct., Dec. 12, 2012, effective Jan. 1, 2013) Interpretation No. 20 [2012] of the Sup. People's Ct. translated by Bei da fa bao (en.pkulaw.cn).

interpretation” on a specific legal issue,¹¹¹ and basically all the Chinese lower courts are supposed to comply with the Supreme People’s Court’s interpretation.¹¹² Therefore, the Supreme People’s Court Opinions and Interpretations are very important legal materials to research in China. The Provision was released by the Supreme People’s Court of PRC in 2012 and took effect January 1, 2013. It interprets some statutes from RCI Regulation in detail and guides the other People’s Court on how to apply the laws to specific cases. For example, the direct infringement liability of ISP, PRC tort law Article 36 does not mention who bears the burden of proof. Should it be the copyright owner or the ISP? Article 4 of the Provision stipulates: “If the network service provider is able to provide evidence . . . the people's court shall support such a claim of the network service provider.”¹¹³ Therefore, according to Article 4, the ISP should bear the burden of proof.

Another issue involving the ISPs’ secondary infringement liability in PRC tort law Article 3 is how to determine whether the ISPs have “actual knowledge” about the infringement activities. Article 9 of the Provision stipulates several factors that should be considered by courts when determining the constructive knowledge of ISPs: “(1) the capability of information administration that an ISP should have based on the nature and mode of services provided by the ISP and the possibility that such services may trigger infringement; (2) type and popularity of the work, performance, and audiovisual recordings disseminated and the degree of the obviousness of the infringement; (3) whether the ISP actively selects, edits, modifies, or recommends the works, performance, and audiovisual

¹¹¹ Zhōnghuá rénmin gònghéguó rénmin fǎyuàn zǔzhī fǎ (中华人民共和国人民法院组织法) [Organic Law of the People's Courts of the People's Republic of China] (promulgated by the St. Council, Jul 1, 1979, amended by the St. Council in Oct 31, 2006) art. 33, para. 1 (China).

¹¹² Organic Law of the People's Courts of the People's Republic of China, art. 33, para. 1: The Supreme People's Court gives interpretation on questions concerning specific application of laws and decrees in judicial proceeding.

¹¹³ The Provision, art. 4: If the network service provider is able to provide evidence that it only provides automatic connection, automatic transmission, information storage space, search, link, file sharing technology and other network services so that it does not contribute to the infringement, the people's court shall support such a claim of the network service provider.

products; (4) whether the ISP has taken positive and reasonable measures to prevent infringement; (5) whether the ISP has set up convenient procedure to receive notifications concerning infringement and respond timely and reasonably to such notifications; (6) whether the ISP has taken reasonable measures against repeated infringing acts committed by the same user; and (7) other relevant factors.”¹¹⁴ The specific case in the next section shows how the Chinese court applies these rules.

B. Case: *China Youth Publishing Group v. Baidu Wenku*,

1. Background

The *Baidu Wenku*¹¹⁵ case is one of the recent copyright infringement cases about Baidu in China. Baidu Wenku is a controversial online document-sharing service provided by the defendant, Baidu Ltd. Baidu Wenku allows its users to share digital documents to the public for online reading. Also, Internet user can earn “points” by sharing digital documents and can use these points to download the digital documents. Since Baidu Wenku went online in 2009, more than 2,700,000 documents were uploaded to its literature section. Most of the documents were uploaded without the copyright owner’s authorization. In March 2011, fifty famous Chinese authors brought a lawsuit together against Baidu. Consequently, Baidu claimed that it started to manually review all the uploaded documents that contain more than one thousand Chinese words from March 26, 2011. By the end of March, document number in Baidu Wenku’s literature section decreased to 150. In September 2011, Baidu closed the

¹¹⁴ The Provision, art 9.

¹¹⁵ Běijīng zhōng qīng wén wénhuà chuánméi yǒuxiàn gōngsī děng zhùzuòquán quán shǔ, qīnquán jiūfēn èrshěn mínshì pàn jué shū (北京中青文文化传媒有限公司等著作权权属、侵权纠纷二审民事判决书) [*China Youth Publishing Group v. Baidu Wenku*], 2014 Gao Min Zhong Zi No. 2045 (Beijing High People’s Ct. Aug 5, 2014).

literature section in Baidu Wenku.¹¹⁶

On December 1, 2011, Wan Juan, who is the author of the book “Kao La Xiao Wu’s English Learning Diary” (Kao’s Diary), granted exclusive right of communication through information network of the book to the plaintiff, China Youth Publishing Group. Kao’s Diary was a popular book and its sales were No. 4 on Amazon.cn in 2012. On January 7, 2011, an Internet user first uploaded Kao’s Diary to Baidu Wenku. Until August 13, 2013, the number of hits of this uploaded file was 245,045. The same files of Kao’s Diary can also be found on Baidu Wenku, which were uploaded by other Internet users from 2011 to 2012.¹¹⁷ The trial court, Beijing First Intermediate People’s Court, held that “Baidu did not fulfill its reasonable duty of care on the use and communication situation of Kao’s diary. It also did not establish an effective copyright protection system. Furthermore, Baidu had fault because it should have known the infringing activities on Baidu Wenku, and the activities of Baidu constituted assist infringement. Therefore, Baidu bears appropriate compensation liability on China Youth Publishing Group’s lost.”¹¹⁸

2. The Plaintiff’s Claims

The plaintiff claimed that (1) the activities of the defendant who provided Kao’s diary in Baidu Wenku directly infringed plaintiff’s right of communication through information network of the book; (2) Although the plaintiff did not sent notification of infringing material to the defendant, Baidu had the subjective fault that it “knows” or “should have known” its infringing activities. Therefore, the activities of the defendant constituted joint-infringement of abetment or assist.¹¹⁹

¹¹⁶ *Baidu Wenku*, at 2-3, Beijing High People’s Ct. Aug. 5, 2014.

¹¹⁷ *Id.*

¹¹⁸ *Id.* at 7.

¹¹⁹ *Id.* at 9.

3. The Defendant's Defense

Baidu claimed that it has already fulfilled its reasonable duty of care as an ISP. Therefore, it should be protected under “safe harbor” doctrine. For example, Baidu developed its own “Anti-piracy DNA comparison recognition system” (fingerprint system), which has been officially online on November 2011. The system automatically compares uploaded files with Baidu's official copyright database. It also blocks the re-uploading activities of infringing documents.

Since the trial court concluded that “In Baidu Wenku homepage's recommendation document section, for most of the documents, its number of hits were merely thousands, which means if document's number of hits reach a certain number, it would be enough to cause attention from Baidu.”¹²⁰ The defendant also claimed, “determining ‘should know’ by the number of hits of the document is lawfully wrong.”

4. The Court's Decision

The appellate court, Beijing High People's Court, believed the main issue of this case is “whether the activities that Baidu use Kao's diary in Baidu Wenku constituted direct-infringement or joint-infringement.”¹²¹ Therefore, the court focused on analyzing (1) whether Baidu constituted direct-infringement and (2) whether Baidu constituted joint-infringement of abetment or assistance.

a. Direct-infringement

On whether Baidu constituted direct-infringement, the court concluded that “according to Article 3 paragraph 1 of the Provision: where a network user or network

¹²⁰ *Id.* at 6-7.

¹²¹ *Id.* at 19.

service provider provides, on an information network, any work, performance, or audio or video recording which a right holder enjoys the right to disseminate on information networks without the permission of the copyright holder, the people's court shall determine that the network user or network service provider has infringed upon the right of dissemination on information networks. . . Therefore, the prerequisite of an ISP constituted direct-infringement is: if the activity that an ISP provide the work exist.”¹²² The court of appeal agreed with trial court’s decision that “Baidu Wenku qualifies the definition of information storage space (see RCI Regulation art. 22), and it was the Internet users who uploaded the infringing document to the server of Baidu Wenku . . . Therefore, the court do not support the plaintiff’s claim that the activities of Baidu uploading infringing documents constituted direct-infringement.”¹²³

b. Joint-infringement

On whether Baidu constituted joint-infringement of abetment or assistance, the court concluded that “according to Article 8 paragraph 1 of the Provision: [t]he people's court shall determine whether a network service provider is liable for infringement as an abettor or aider according to the fault of the network service provider. The fault of a network service provider means whether the network service provide knows or should have known a network user's infringement of the right of dissemination on information networks. . . Therefore, the prerequisite of an ISP bear joint-liability by its network users using its service to implement infringement is that, the subjective fault that an ISP ‘knows’ or ‘should have known’ the infringing activities.”¹²⁴

Article 8 paragraph 3 of the Provision stipulates: “where a network service provider is able to prove that it has taken reasonable and effective technical measures but it is still

¹²² *Id.* at 21.

¹²³ *Id.*

¹²⁴ *Id.* at 21-22.

difficult for it to discover a network user's infringement of the right of dissemination on information networks, the court shall determine that the network service provider is not at fault.” Article 9 of the Provision also stipulates seven factors on how to determine whether an ISP should have known an infringement was occurring. Based on these two rules, the court analyzed whether Baidu was at subjective fault for ‘knowing’ or ‘should have known’ the infringing activities in five factors. This five-factor test is similar to a red flag test in *YouTube*, including similar rationale from the objective and subjective standard, and something more standard. The next section introduce the red flag test¹²⁵ in Baidu, which is called the “should have known” rule.¹²⁶

5. “Should have known” rule

Similar to the red flag test in *YouTube*, the court applied a five-factor test on whether Baidu should have known the infringing activities on its network. First, on whether Baidu had subjective fault of “should have known” because Kao’s diary was a popular book, the court concluded “even though the ISP knows the sales information about the book, if the ISP filter its information storage space by limited key words, such as author’s name or work’s name, it is possible that the dissemination of fair use of the work might be limited, such as comments or thoughts of the book, which is harmful to information communication and sharing.”¹²⁷

Second, on whether Baidu had subjective fault of “should have known” because it actively selected, classified, edited, and sorted out uploaded documents, the court concluded “the purpose of setting classified section on Baidu Wenku is to provide convenience for public to search or access information . . . There is no evidence to proof that Baidu had

¹²⁵ *Id.* at 15.

¹²⁶ *Id.* at 22.

¹²⁷ *Id.*

actually accessed the content of Kao's diary."¹²⁸

Third, whether Baidu directly obtained economic benefit from its network users' uploading activities therefore constituted abetment infringement. Article 11 paragraph 1 of the Provision stipulates: "where a network service provider directly gains economic benefits from the work, performance, or audio or video recording provided by a network user, the people's court shall determine that the network service provider has a higher duty of care for the network user's infringement of the right of dissemination on information networks." According to paragraph 1, the court held that whether Baidu directly obtained economic benefit from its network users' uploading activities, is a factor to determine whether Baidu has a higher duty of care. It is not a prerequisite to determine whether Baidu's activity constituted abetment joint-infringement."¹²⁹

Article 11 paragraph 2 of the Provision stipulates: "if a network service provider gains benefits from inserting advertisements into a specific work . . . it shall be determined that the network service provider directly gains economic benefits as mentioned in the preceding paragraph, however, excluding the general advertising and service charges, among others, collected by a network service provider for providing network services." The court holds that "reading infringing document of Kao's diary in Baidu Wenku is free, therefore Baidu did not gain economic benefits directly from the infringing document . . . Baidu obtained the use of right of the uploaded work from 'Wenku Agreement' (an uploader have to sign it before sharing). It only gains the possibility of future profit instead of actual direct economy benefits."¹³⁰

Fourth, on whether the "points reward system" of Baidu Wenku constituted abetment infringement, the court concluded that "the point reward system is a business modal of Baidu

¹²⁸ *Id.* at 23.

¹²⁹ *Id.* at 24.

¹³⁰ *Id.*

Wenku. Its main purpose is to encourage network users sharing documents and using Baidu Wenku. From a business perspective, the point reward system facilitates user loyalty . . . and points are not directly related to economy benefits.” Therefore, the points reward system did not indicate subjective intention of abetment infringement.

Fifth, Baidu explained the reason why documents appeared on Baidu Wenku homepage’s recommendation document section is that these “recommend” documents were authorized by the copyright owners. A document’s number of hits is not a factor for its placement in the recommendation section. The court believed that “the aforementioned fact at least proves: Baidu do know which documents were authorized by copyright owners; Baidu was able to know the number of hits of the documents. Therefore, Baidu should pay reasonable attention on the documents that were not under copyright owner’s authorization and the number of hits has reached a certain high quantity.”¹³¹ It further ruled “however, from the first infringing document was uploaded in January 17, 2012, until August 13, 2013 . . . for more than one year, Baidu did nothing to stop the dissemination of infringing document. Such activity shall not be recognized as actively fulfilling its legal duty.”¹³²

The appellate Court upheld the trial judgment that “Baidu only need to pay ordinary duty of care as a normal reasonable person. It is easy to find that the possibility is extremely low for the related document obtaining authorization, therefore it is highly possible that the related document might infringe copyright.”¹³³ After supporting aforementioned trial court’s holding, the court further supplied that “when an information space service provider knows that related documents are not authorized by copyright owner and the number of hits is high, it has a high duty of care. The ISP should actively try to contact the uploader, verify if the related documents are original or under legal authorization. It should adopt effective

¹³¹ *Id.* at 25.

¹³² *Id.*

¹³³ *Id.*

measures to prevent infringement from happening or sustaining.”¹³⁴

As a conclusion from the appellate Court’s decision, the should have know rule actually adopted the similar rationale from the subjective and objective standard from *YouTube*. First, the court determined that Baidu subjectively knew the fact that the infringing document on its network was popular and unauthorized. Second, the fact that the number of hits of the infringing document has reached a certain high quantity, which was objectively obvious enough for Baidu, as a normal reasonable person, to pay a reasonable duty of care on the infringing document.¹³⁵ Furthermore, the appellate Court required that the ISP should actively verify the document and adopt effective measures to prevent infringement, which is similar to something more standard in *YouTube*. The next section analyzes ISP’s reasonable duty of care requirements.

6. ISP’s reasonable duty of care

Similar to something more standard in *YouTube*, which requires an ISP to take active steps to prevent copyright infringement on its network, according to Article 8 paragraph 3 of the Provision, ISP’s reasonable duty of care requires ISP to adopt “reasonable and effective technical measures” to “discover a network user’s infringement . . .” The appellate court did not discuss what kind of reasonable and effective technical measures an ISP should adopt, and it also did not mention whether Baidu’s fingerprint system qualified as a reasonable and effective technical measure. Therefore, a serious problem for ISP in China is that: what measure should an ISP adopt to fulfill a reasonable duty of care?

In this case, Baidu claimed that it had fulfilled its reasonable duty of care by adopting several technical measures. The core measure is Baidu’s fingerprint system. It automatically

¹³⁴ *Id.*

¹³⁵ *Id.*

compares uploaded files with Baidu's official copyright database. Thus, the system will block the uploading process if it finds the uploading file matches an official file in the database. However, not many copyright owners are willing to provide their official works to Baidu.¹³⁶

The trial court discussed this issue and believed that the fingerprint system functions as a comparison of the copyright content's fingerprint, however, the ISP does not have effective access to obtain copyright content. Therefore, it is not appropriate to require the ISP to filter, block, or delete a file because of a famous work. Such an obligation is also not beneficial for social development and cultural prosperity.¹³⁷

The trial court did not consider the fingerprint system to be a reasonable and effective technical measure from a social perspective. From a technical perspective, the fingerprint system is not reliable because an Internet user can easily circumvent the system by modifying the fingerprint of the digital file. For example, MD5 Message-Digest Algorithm (MD5) is one of the most common algorithms to generate fingerprints of a digital file. Each digital file has a unique MD5 code except an exact copy of the file. Therefore, a MD5 code is considered as a fingerprint of a digital file. By comparing the MD5 code of an uploading file to all the MD5 codes in the official copyright database, the fingerprint system can verify whether the uploading file matches an official copyright work in the database.

However, the fingerprint of a digital file is not exactly the same as human being's fingerprint. A human being is not able to change its fingerprint, while the fingerprint of a digital file can easily be changed. By modifying the digital information, such as size, type, quality, etc., an Internet user is able to upload a file that has a different fingerprint with an official copyright work, but has almost the same content. Therefore, the fingerprint of a digital file is similar to an identification code. Each digital file has its own unique

¹³⁶ *Id.* at 16.

¹³⁷ *Id.* at 5-6.

identification number, unless it is the exact copy of a digital file. Even two very similar digital files with only slight differences between them will have different identification codes.

In conclusion, the fingerprint system is not able to effectively identify infringement even with an official copyright database. For example, if a user wants to upload a popular movie “Star Wars” to a Cloud without the copyright owner’s authorization, then the ISP may cooperate with the copyright owner of the movie and obtain the fingerprint of the file, and the user may fail to upload the movie because of the fingerprint system. However, the user can easily search and access the information on the Internet about how to modify a digital file’s fingerprint. With sample technology tools, a three-hour movie can be modified to two hours and fifty-nine minutes; a MP4 file can be modified to AVI file; the video quality of 1080P can be modified to 720P. A little change on a modified file changes the fingerprint of a digital file. Such little modification does not affect the normal use of a movie file, but the fingerprint system cannot identify a modified file as an infringing material because it has a different fingerprint.

From both a social and technical perspective, the fingerprint system is not a reasonable and effective technical measure for an ISP to fulfill its reasonable duty of care. What technical measures an ISP should adopt remains an unsolved issue. However, with technological innovation, a reasonable solution may emerge in the future. The specific solution proposal will be discussed in Chapter VI.

7. Paradox for ISP

As an intermediary between the Internet user and copyright owner, ISP is facing a paradox about copyright protection because both proactive and passive requirements exist in ISP policy. According to safe harbor doctrine and the notice-and takedown provision, an ISP should remain passive-reactive to obtain immunity when copyright infringement occurs on

their service. The more active ISPs are in the hosting or transmission process, the less likely they are to be protected by safe harbors.¹³⁸ However, the copyright owner and legislature also requires ISP to do something more than stay under the safe harbor protection. For example, Article 9 of the Provision stipulates: “The people's court shall determine whether a network service provider should have known an infringement based on . . . (4) Whether the network service provider has proactively taken reasonable measures to prevent infringement.”¹³⁹ Such paradoxical arrangement requires ISP to act both actively and passively on copyright protection, which is unsustainable under the current online environment.¹⁴⁰

The paradox actually appears in this Baidu Wenku case. Neither trial court nor Appellate court mentioned Article 8 paragraph 2 of the Provision: “Where a network service provider fails to conduct proactive examination regarding a network user's infringement of the right of dissemination on information networks, the people's court shall not determine on this basis that the network service provider is at fault.”¹⁴¹ However, after holding that Baidu should pay a reasonable duty of care on the number of hit of Kao’s diary, the court also required that the ISP should actively try to contact the uploader and verify if the related documents are the original or under legal authorization. The ISP should adopt effective measures to prevent infringement from happening or sustaining. The Provision provides that the ISP is not obliged to conduct proactive examination on its network, while the court requires an ISP to actively contact the uploader and verifying the documents. Such paradoxical requirement shows a serious problem: whether an ISP should actively involve into copyright protection. This question will be further discussed in Chapter V.

¹³⁸ JEREMY & CHRISTOPHER, *supra* note 2, at 405.

¹³⁹ The Provision, art. 9(iv).

¹⁴⁰ JEREMY & CHRISTOPHER, *supra* note 32, at 405.

¹⁴¹ the Provision, art 8.

C. Japan's New Approach to ISPs' Copyright Liability

1. Statutes

a. Japanese Copyright Law

Japan enacted its first Copyright Act in 1899.¹⁴² Later, the 1899 Copyright Act was revised in 1970, and was superseded by the current 1970 Copyright Act.¹⁴³ Similar to the Chinese Copyright Law, Article 23 of the Japanese Copyright Act provides “[t]he author of a work has the exclusive right to transmit to the public that work (this includes the right to make the work available for transmission, if the work is to be transmitted to the public via automatic public transmission).”¹⁴⁴ To adapt to the digital-network age, the Copyright Amending Act was promulgated on January 19, 2009, and came into effect on January 1, 2010. Some provisions have been amended responding to the needs of digital environment, including ISPs. For instance, Article 47 paragraph 6 of the Copyright Act¹⁴⁵ provides a “safe harbor” for ISPs that provide search engine services on Internet. The prerequisites for ISPs to copy copyrighted works are that: (1) the ISPs collect, copy and store the website data from Internet to their own servers by an automatic Web crawler¹⁴⁶ program in advance; (2) the ISPs copy or modify the data by keywords; (3) in response to search requests from users, the ISPs display the URL and part of the description or images of the website relating to the keyword as search results, which are stored on the ISPs’ servers.¹⁴⁷ To prevent online copyright infringement, ISPs are not allowed to provide the search results if the ISPs “know that making such a recording available for transmission constitutes a copyright

¹⁴² Chosakkun Ho [Copyright Act] Act No. 39 of 1899 (Japan).

¹⁴³ Chosakkun Ho [Copyright Act] Act No. 48 of 1970 (Japan).

¹⁴⁴ Chosakkun Ho [Copyright Act] Act No. 73 of 2009 (Japan), art. 23, para. 1 (Japan) English translation are available at <http://www.japaneselawtranslation.go.jp/law/detail/?id=2506&vm=04&re=02&new=1>.

¹⁴⁵ Copyright Act, art. 47, para. 6. Act No. 73 of 2009 (Japan).

¹⁴⁶ Also called “spidering software.” The program can copy all the pages it visit for later processing by a search engine which indexes the downloaded pages so the Internet users can search much more efficiently.

¹⁴⁷ Heisei 21-nen chosakukenhō kaisei no pointo (Points on 2009 Copyright Act Amendment) <http://dan-law.jp/commentary/H21Copyright-Commentary.pdf> (last visited Oct. 2, 2016).

infringement.”¹⁴⁸ Compared with the safe harbor doctrine in China and the U.S., the Japanese Copyright Act provides a similar safe harbor construct.

b. Limitation of Provider Liability Act

Article 3 paragraph 2 (ii) of the Limitation of Provider Liability Act stipulates a “notice and takedown” provision for ISPs. This provision is slightly different from the strict notice-and-takedown regime, which provides “a somewhat more subscriber friendly system of ‘notice-wait-and-takedown’.”¹⁴⁹ Upon the notification of a copyright owner, the Chinese notice-and-takedown provision requests that the ISP “promptly removes the works . . .”¹⁵⁰ and the U.S. notice-and-takedown provision requests the ISP “respond[] expeditiously to remove . . . the material . . .”¹⁵¹ While in the Japanese provision, the statute grants the alleged infringer seven days to respond before its content is taken down.¹⁵² After the ISP received notification from the copyright owner, the alleged infringer is notified by the ISP and offered the opportunity to contest the claim of infringement. If the alleged infringer agrees to have the material removed, or no counter notice is received within seven days, the content is removed from the ISP’s host system.¹⁵³

Compare with the strict notice-and-takedown regime in China and the U.S., the Japanese adopts a friendly attitude on ISP-related provisions. Moreover, the Japanese court also adopts a non-strict attitude on ISP-related cases. In *Winny*, the Japanese Supreme Court does not impose strict liability on the P2P software provider. The Japanese Supreme Court’s decision indicates that Japan follows the traditional passive-reactive ISP model. The Detail discussion of the *Winny* case will take place in the next section.

¹⁴⁸ Copyright Act., art. 47, para. 6. Act No. 73 of 2009 (Japan).

¹⁴⁹ JEREMY & CHRISTOPHER, *supra* note 32, at 387.

¹⁵⁰ Regulations for the Protection of the Right of Communication through Information Network, art. 22.

¹⁵¹ 17 U.S.C. § 512(c)(3).

¹⁵² Limitation of Provider Liability Act, art. 3, para. 2 (ii).

¹⁵³ JEREMY & CHRISTOPHER, *supra* note 32, at 387.

2. Case: *Winny*

a. Background

In May 2002, the accused, Isamu Kaneko, developed and released a program called “Winny.” Winny is a file-sharing software program sends and receives data with the applied use of P2P technology by which a network of computers is formed in a manner that individual computers act equally, with no central server involved.¹⁵⁴ It can also keep its users' identities untraceable. The accused was a former researcher in the computer science department at Japan's prestigious Tokyo University. He released the program for free through his own website and Japan's infamous anonymous forum 2Channel (“2ch”). Kaneko made announcements about the program, including updates of the software, on 2ch's file sharing sub forum, which is widely known for copyright violations. By 2006, three million people had used Winny and the program has become one of the most widely used P2P software in Japan.¹⁵⁵ Though Winny could be used to distribute material legally, it was widely used to distribute copyrighted material without the copyright owner's consent.

b. The trial court decision

The trial court believed that whether it is unlawful to provide such technology to others depends on (1) the actual situation of the use of the technology in society; (2) the provider's perception of such a situation; (3) the provider's subjective views upon provision.¹⁵⁶ The

¹⁵⁴ Saikō Saibansho [Sup. Ct.] Dec. 19, 2011, 2009 (A) No. 1900, 65 SAIKO SAIBANSHO KEIJI HANREISHU [KEISHU] 1-2, <http://www.courts.go.jp/hanrei/pdf/20111221102925.pdf>. The Court's English translation can be accessed at <http://www.courts.go.jp/english/judgments/text/2011.12.19-2009.-A-.No.1900.html>.

¹⁵⁵ Ridwan Khan, *Pure Software in an Impure World? WINNY, Japan's First P2P Case* 8 E. ASIA L. REV. 21, 24 (2013).

¹⁵⁶ *Winny*, [Sup. Ct.] Dec. 19, 2011, at 3-4.

court found the accused knew the actual situation of the use of file-sharing software programs and held that the act of the accused can be regarded as constituting accessoryship and found the accused guilty of accessoryship to the crime of violation of the Copyright Act, and rendered a judgment sentencing the accused to a fine of 1.5 million yen.¹⁵⁷

c. The Court of Appeals decision

The appellate court, Osaka High Court, believed that providing a value-neutral software program on the Internet has made it easy for the user to commit the criminal act. It is not sufficient that the provider of the software program perceives and accepts the possibility or probability that someone among many and unspecified persons would engage in an unlawful activity with the use of the software program. However, accessoryship should be established only in the case where the provider has gone further to provide the software program while recommending others to use it exclusively or mainly for the purpose of engaging in an unlawful activity. Consequently, the court did not find that the accused went further to provide the alleged software while recommending others to use them exclusively or mainly for the purpose of infringing copyright. Accordingly, the court concluded that the accused could not be found guilty of accessoryship and pronounced the accused not guilty.¹⁵⁸

3. The Japanese Supreme Court's opinion on *Winny*

In a four to one decision, the Japanese Supreme Court affirmed the appellate court's decision. However, the Supreme Court ruled that the appellate court erred in construing the Provision of Article 62 paragraph 1 of the Penal Code: "A person who aids a principal is an accessory."¹⁵⁹ First, the court believed that although Winny could be used for a legitimate

¹⁵⁷ *Id.* at 3.

¹⁵⁸ *Id.* at 4-5.

¹⁵⁹ Kei Hou [Penal Code] Act No. 54 of 2007, art. 6 para. 1 (Japan). English version are available at

or an unlawful purpose, it is the program users who decide how to use Winny, not its software provider. The majority considered the act of the accused's releasing the program online as "a rational approach" to the software's development.¹⁶⁰

The court further pointed out that "to avoid causing an excessive chilling effect to activities for developing such software programs, providing a software program should not be regarded as constituting an act of aiding copyright infringement only because there is a general possibility that the software program would be used for the purpose of infringing copyright . . ." ¹⁶¹ Such a standpoint is similar to the rationale in *Grokster*, which requires a certain test to determine whether a software constitutes an act of aiding copyright infringement.

The court provided its test, which is similar to a red flag test including the objective and subjective standard in the *YouTube* and *Baidu* case:

the provider's act of releasing and providing the software program should be regarded as constituting an act of aiding copyright infringement only in the case (i) where a person has released and provided a software program while perceiving and accepting a specific and immediate risk of copyright infringement to be committed with the use of the software program, and such copyright infringement has actually been committed and (ii) where in light of the nature of the software program, the objective situation of use of the software program, and the method of providing it, it is highly probable that among those who acquire the software program, a wide range of persons will use the software program for the purpose of infringing copyright, to a level where their use cannot be tolerated as exceptional, the provider has released and provided the software while perceiving and accepting such high probability, and the principal has actually committed copyright infringement with the use of the software program.

In other words, the red flag test in Japan determines: (1) whether the ISP subjectively perceive a specific and immediate risk of copyright infringement; (2) whether the ISP perceives that the objective situation of the infringing activities cannot be tolerated as exceptional. In sum, similar to the U.S. and China, Japan has also adopted an objective and subjective standard to

<http://www.japaneselawtranslation.go.jp/law/detail/?id=1960&vm=04&re=01&new=1>

¹⁶⁰ *Winny*, [Sup. Ct.] Dec. 19, 2011, at 6.

¹⁶¹ *Id.*

determine whether the ISP has actual knowledge on infringement action and whether the ISP has subjective fault on providing the network service. Chapter V provides further comparison of the objective and subjective standard in three countries.

Next, the court applied this test to several facts against the accused and concluded that when the accused released and provided Winny: (i) There is no specific and immediate risk of copyright infringement; (ii) There is no evidence to show the objective situation of the use of Winny; (iii) From a subjective view, there is no sufficient evidence to find that the accused perceived the number of people who would use Winny for the purpose of infringing copyright had increased to a level where their use cannot be tolerated as exceptional.¹⁶² On the other hand, although the accused knew that some users might use Winny for the purpose of copyright infringement, he could not have known that the illegal usage had grown so much that he could be imposed with strict liability. Therefore, the court held that the accused lacked the intent of accessoryship to the crime of violation of Copyright Act.¹⁶³

In the dissent, Justice Otani agreed with the majority opinion that the accused shall be punished “only if the act of providing is performed in the situation where there is a specific and higher level of probability that the principal will use the software program in an infringing manner.”¹⁶⁴ However, he did not agree with the majority opinion on the application of the facts. For example, there is evidence from the trial court shows that at least forty percent of the files flowing on the Winny network were copyrighted works and these works were exchanged among users without copyright owners’ authorization.¹⁶⁵ Justice Otani believed the evidence obviously shows that (1) the accused had perceived and accepted the objective situation concerning the high probability of infringing use,¹⁶⁶ (2) the accused

¹⁶² *Id.* at 8.

¹⁶³ *Id.* at 10.

¹⁶⁴ *Id.* at 11 (Justice Otani, dissenting).

¹⁶⁵ *Id.* at 10.

¹⁶⁶ *Id.* at 15 (Justice Otani, dissenting).

had the intent of aiding.¹⁶⁷ Although the accused did not have a positive intent of infringement, he engaged in developing and providing the software program, which was mainly designed for the purpose of the efficient exchange of a variety of digital files for a large range of people while maintaining secrecy of communications. Moreover, after the accused knew about the illegal use of Winny, he “still engaged in the act of providing without taking any measures to check the infringing use . . .”¹⁶⁸ In sum, Justice Otani concluded that the majority overvalued the accused’s intent and the evidence was sufficient enough to prove the intent of aiding infringement.

4. Inducement analysis

Both the majority opinion and the dissent of the court focus on the issue of contributory infringement instead of inducement infringement. Article 61 paragraph 1 of the Penal Code stipulates: “A person who induces another to commit a crime shall be dealt with in sentencing as a principal.” In the dissent, Justice Otani concluded two major points to examine whether a user will use Winny for the infringing manner. (1) Whether Winny can be easily used for infringing copyright and is likely to induce infringement; (2) Whether there are any means to check infringement.¹⁶⁹ However, Justice Otani did not go further in inducement analysis.

In the *Grokster* case, the U.S. Supreme Court held that the P2P software provider bears secondary liability under inducement theory. While in *Winny*, the accused did not aim at revenue, and the majority believed the accused intended to build a P2P network. However, it could be that the accused simply wanted more people to use Winny to build and test his work. After the accused knew that the number of the infringing users is increasing, although he did not intent to encourage copyright infringement, the increasing number of Winny users

¹⁶⁷ *Id.* at 17 (Justice Otani, dissenting).

¹⁶⁸ *Id.*

¹⁶⁹ *Id.* at 12 (Justice Otani, dissenting).

actually fulfilled his intention. Therefore, the accused perceived that the number of Winny users was increasing because Winny can be used in an infringement manner. The infringing feature of Winny kept attracting people to use it, but the accused did nothing to stop it because his intent was to encourage more people to use Winny.

5. Summary

As Justice Otani concluded in the dissent, the case may bring a chilling effect on technological innovation if the software developer was punished by secondary liability. However, “as long as the developer of technology intends to provide the technology widely in society with no limit to users, he should proceed with development while giving due consideration to this aspect, as his responsibility in society as a developer.”¹⁷⁰ Such a standpoint can also be found in the *Baidu* case, which requires that an ISP should pay reasonable duty of care on copyright infringement. In sum, the Japanese Supreme Court requires an ISP to stay on a passive-reactive position instead of an active-preventive position. The next chapter analyzes the legal theories and cases in regarding to ISPs and compares two different approaches to the ISP model.

¹⁷⁰ *Id.* at 20 (Justice Otani, dissenting).

Chapter V

Comparative analysis: The U.S., China, and Japan

This Chapter comparatively analyzes ISP legal theories and cases among the U.S., China and Japan, and examines why Japan maintains a passive-reactive ISP approach while China and the U.S. choose an active-preventive approach. This chapter focuses on the legal challenge of ISP in China, especially Baidu, and explores why China should follow the active-preventive trend using legal experience from the U.S. and Japan.

A. Similarities among the U.S., China and Japan

As mentioned above in Chapter III and IV, the U.S., China and Japan adopted similar ISP legal models in their legislative branches, including the safe harbor doctrine, the notice-and-takedown provision, and the red flag provision.¹⁷¹ With regard to digital distribution rights of copyright owners, all of these three countries enacted public performance rights in their Copyright Law.¹⁷² According to the facts from *YouTube*, *Baidu*, and *Winny*, although the users of ISPs are the direct copyright infringers who upload the infringing materials to ISPs' networks, the copyright owners sued ISPs for secondary infringement liabilities because suing unspecific individuals are costly and time-consuming. In determining whether the ISPs bore secondary infringement liabilities on its network users' behavior, courts from three jurisdictions adopted similar two-prong tests. (1) The actual knowledge test: whether the ISP has actual knowledge about the infringing actions on their networks; (2) The red flag test: whether the fact of infringing activity is obvious enough to a

¹⁷¹ JEREMY & CHRISTOPHER, *supra* note 32, at 377-378.

¹⁷² 17 U.S.C. §106(4): Public performance right; Japanese Copyright Act, art. 23: Right to transmit to the public; Copyright Law of the PRC, art. 10(xii): Right of dissemination through information network.

reasonable person. The actual knowledge test requires an ISP to have constructive knowledge of specific and identifiable infringements of individual items instead of general and vague knowledge about the infringement. The red flag test consists of two prongs: the subjective and objective standard. Courts from these three jurisdictions have adopted similar red flag tests, including the subjective and objective standard.

In the U.S., the Second Circuit pointed out in *YouTube* that the subjective standard refers to whether the ISP is aware of the actual knowledge of specific infringement on its network, and the objective standard refers to whether the infringement fact is apparent enough to a reasonable person.¹⁷³ The Ninth Circuit further pointed out that in determining whether the ISP was aware of a red flag, a subjective standard should be applied first. In deciding whether the subjective facts constitute a red flag, an objective standard should be used.¹⁷⁴ Courts in Japan and China had different expressions but the same rationale on the subjective and objective standard. In China, the subjective standard refers to whether the ISP knows a network user's infringement,¹⁷⁵ and the objective standard refers to whether the ISP should have known a network user's infringement "based on a clear fact."¹⁷⁶ In *Baidu*, the Beijing High People's Court analyzed five facts and decided that one fact triggered the subjective and objective standard: (1) Baidu subjectively knew the fact that the infringing document on its network was popular and unauthorized. (2) The number of hits of the infringing document had reached a certain high quantity, which was objectively obvious enough for Baidu to pay a reasonable duty of care on the infringing document.¹⁷⁷ In Japan, as the Japanese Supreme Court pointed out in *Winny*, the subjective standard refers to whether

¹⁷³ *Viacom*, 676 F.3d at 31.

¹⁷⁴ *UMG Recordings, Inc. v. Shelter Capital Partners LLC*, 718 F.3d 1006, 1026 (9th Cir. 2013).

¹⁷⁵ The Provision, art. 8: . . . The fault of a network service provider means whether the network service provide knows or should have known a network user's infringement of the right of dissemination on information networks.

¹⁷⁶ The Provision, art. 9.

¹⁷⁷ *Baidu Wenku*, at 25, Beijing High People's Ct. Aug 5, 2014.

the ISP¹⁷⁸ subjectively perceives a specific and immediate risk of copyright infringement; and the objective standard refers to whether the ISP perceives that the objective situation of the infringing activities cannot be tolerated as exceptional.¹⁷⁹ In sum, all the ISPs claimed that although they had general knowledge about the infringing activities on their network, they did not have constructive knowledge of specific and identifiable infringements of individual items. Therefore, all the courts applied similar red flag tests to determine whether the ISPs bore the secondary liabilities. And all the red flag tests included a similar rationale: the subjective and objective standard.

After applying the similar red flag tests, China and the U.S. adopted an active-preventive approach, which required ISPs to take active steps to prevent copyright infringement on its network. While in Japan, the majority of the Japanese Supreme Court maintained a traditional passive-reactive ISP approach and decided that the ISP was not guilty because he had no intention on copyright infringement.¹⁸⁰ In the dissent, Justice Otani criticized the majority's opinion and demonstrated that a technology developer was responsible to give due consideration on its product.¹⁸¹ The next section discusses two questions about these two different approaches: why different countries adopted the opposite ISP approaches and which approach provides better solutions to the ISP issues in China.

B. The difference between the U.S., China and Japan

1. Different ISP approach - passive-reactive vs. active-preventive

In *YouTube*, *Baidu* and *Winny*, even though three courts from different jurisdictions applied their own ISP-related rules, the courts adopted similar tests as to whether ISP has

¹⁷⁸ This thesis adopts a broad definition of ISP. Therefore in *Winny*, the P2P software provider is considered an ISP.

¹⁷⁹ *Winny*, [Sup. Ct.] Dec. 19, 2011, at 6.

¹⁸⁰ *Id.* at 10.

¹⁸¹ *Id.* at 20 (Justice Otani, dissenting).

actual knowledge about copyright infringement on their network. However, after applying the test, courts adopted different rules on their decisions, which reflected different approaches to their ISP policies in these three countries. In *Winny*, the Japanese Supreme Court applied the Penal Code to test whether the ISP has the intention to aid infringement action. The majority believed the software provider did not have the intention and found the accused not guilty.¹⁸² This decision indicated that Japan adopted a traditional passive-reactive approach to ISP model. Justice Otani argued in the dissent that the evidence was sufficient to prove the software provider's actual knowledge on infringing activities, and therefore the ISP should take active steps to prevent infringement.¹⁸³ Like what Justice Otani suggested in the dissent, the courts in China and the U.S. adopted a more active-preventive approach on ISP cases.

In *YouTube*, after applying the objective and subjective standard, the Second Circuit suggested that ISP should do something more than passively remove or block access to materials posted on its website.¹⁸⁴ Such a standard requires an ISP to play a more active-preventive role in copyright protection. In *Baidu*, the Beijing High People's Court required the ISP to pay reasonable duty of care about the material on its network. The main reason why Japan did not follow this trend is that the Japanese Supreme Court worried that putting ISPs into an active-preventive role might cause a chilling effect on technological innovation because ISPs may lose the incentive to provide a better service.¹⁸⁵ The Japanese Supreme Court had to make a decision with regard to its own national circumstance. As a well-developed country in both technical and economic areas, the business market of ISPs in Japan is limited. Requiring ISPs to bear more obligations means more expense on their business. Therefore, ISP companies in Japan may lose interest in technological innovation. However, the Internet business market in China is totally different. The issue is whether the

¹⁸² *Winny*, [Sup. Ct.] Dec. 19, 2011, at 10.

¹⁸³ *Id.* at 20 (Justice Otani, dissenting).

¹⁸⁴ *Viacom*, 676 F.3d at 38.

¹⁸⁵ *Winny*, [Sup. Ct.] Dec. 19, 2011, at 6.

ISPs in China would stop technological innovation if they have to bear more obligations on copyright protection.

First, unlike Japan, the Internet market is rapidly growing in China. As mentioned in Chapter III, the number of Chinese Internet users was about 668 million in 2015, and the penetration rate reached 50.3%, up 2.4 percentage points from the end of 2014.¹⁸⁶ The population of China is more than 1.4 billion, therefore the Chinese Internet market has grown very fast in recent years. Secondly, technological innovation is the key for tech-companies. ISPs have to keep providing better online services to keep up their market, and they can only provide better services by technological innovation. Thirdly, the ISP market is highly competitive, so tech-companies are not able to survive without technological innovation. For example, after Google left China,¹⁸⁷ Baidu occupied most of the search engine market in China because it provided a better search engine service in Chinese. “Baidu is reaping the benefits of Google's ban in China—and of course, a massive and growing Internet user population—increasing its share to 8.8% of search ad spending globally this year, up from 7.6% in 2014.”¹⁸⁸ If Baidu stops innovating online technology or providing a better online service, other ISPs in China would be occupied Baidu’s business market immediately. As a business company, losing ground in the business market is unacceptable for any ISPs in China. As a conclusion, an active-preventive ISP model may cause a chilling effect on technological innovation because it requires ISPs to bear more obligations on copyright protection, but ISPs in China would not stop technological innovation or providing a better online service.

A more active-preventive ISP model may provide a better copyright protection than a traditional passive-reactive model in China. As mentioned in Chapter I, from 2011 to 2014,

¹⁸⁶ CNNIC, 37th Statistical Report on Internet Development in China, *supra* note 93, at 1.

¹⁸⁷ Helft & Wines, *supra* note 91.

¹⁸⁸ EMARKETER, *supra* note 92.

Baidu has repeatedly been sued more than 40 times for copyright infringement by different copyright owners over the world.¹⁸⁹ The traditional passive-reactive model in China has been proved unsuccessful to solve Baidu issue in China. In 2014, The Beijing High People's Court provided an active-preventive approach in *Baidu* to solve this issue. However, unlike the U.S., case law in China is not able to establish precedent. The next section compares the different legal systems among the U.S., Japan and China, and discusses how to reform an active-preventive ISP model in China for better copyright protection.

2. Different legal systems – common law vs. civil law

As a common law country, most of the ISP secondary liability theories in the U.S. were established by cases. By contrast, China and Japan, as two civil law countries, rely on their codes rather than case law because cases are not bound in their courts. In the 21st century, the paradox is that network technology developed very fast, but the development of tech-related law is always slower than technology. For example, the DMCA was enacted before 2000 when UGC and Cloud did not even exist. Although new legal issues appear with new technologies, the U.S. courts were able to create new precedents to follow technological innovation. On the contrary, a civil law country like China has to keep updating its tech-related laws to follow the step of technological innovation. However, the paradox still exists because it usually takes more than two years to amend a law, while new technologies may emerge tomorrow. Since the ISP cases in the U.S. are comparatively updated, China can learn the rationale and experience from the latest ISP cases in the U.S.

Like China, Japan is also a civil law country. Although case law is not bound in Japan, all the Japanese lower courts are supposed to comply with the Japanese Supreme Court's

¹⁸⁹ Zhang, *supra* note 3, at 29.

case.¹⁹⁰ In *Winny*, the Japanese Supreme Court decided its first P2P software case by the Penal Code. As such, Japanese courts may follow the Supreme Court's decision on new technological legal issues. In China, case law is not bound in any Chinese courts. According to Article 33 of the Organic Law of the People's Courts of the People's Republic of China,¹⁹¹ the Supreme People's Court provides interpretations on specific legal issues, and all the Chinese lower courts are supposed to comply with the Supreme People's Court's interpretation (hereinafter "judicial interpretation"). The Supreme People's Court may provide a judicial interpretation to solve specific legal issues. Thus, the judicial interpretation is usually more updated than the tech-related law in China. In *Baidu*, the Beijing High People's Court highly relied on the Provision to analyze the case. Therefore, judicial interpretation is considered a practical legal solution to the new technology issue in China.

3. The active-preventive trend in China

The ISP related law is supposed to balance the interest among ISPs, copyright owners and network users. If a more active-preventive ISP model may fulfill this purpose, the legislature should follow this trend and impose more duties on ISPs. In the Provision, the Supreme People's Court requires ISPs bear reasonable duty of care with infringement materials on its network. In *Baidu*, the Beijing High People's Court also followed this rationale and decided that although Baidu neither directly infringed copyright nor indirectly aiding its users infringed copyright, it should still pay reasonable duty of care if the number of hits of the infringing material has reached a certain high quantity.¹⁹² Although the judicial

¹⁹⁰ See Minji soshō-hō [Code of Civil Procedure] Act No.36 of 2011, art. 318, para. 1 (Japan). English translation is available at <http://www.japaneselawtranslation.go.jp/law/detail/?id=2092&vm=04&re=02&new=1>.

¹⁹¹ Organic Law of the People's Courts of the People's Republic of China, art. 33, para. 1: The Supreme People's Court gives interpretation on questions concerning specific application of laws and decrees in judicial proceeding.

¹⁹² *Baidu Wenku*, at 25, Beijing High People's Ct. Aug 5, 2014.

branch in China has followed new trend, both judicial interpretation and case law are not bound in China. Chinese courts do not have to follow the new active-preventive ISP approach, which may create uncertainty about ISP issues in China. For example, different Chinese courts may adopt opposite approaches to the ISP cases that have similar facts. In conclusion, to provide consistency on the ISP model in China, the Chinese legislature should follow the trend from the judicial decision and enact an active-preventive ISP model into Chinese Law. However, in order to enact an active-preventive ISP model in China, at least two major problems exist in current Chinese law: lack of ISP definition and legal conflict with current passive-reactive statutes. The next section analyzes these two problems and proposes solutions for legal reform.

C. The Potential Problems Lurking in the active-preventive ISP model

1. Definition of ISP

As mentioned in Chapter II, Chinese Law has no specific definition of ISP, which may bring obstacles to facts finding and judicial decisions. In Chinese case law, Judge Zhou Xiaobin of the Beijing Second Intermediate People's Court drew the conclusion from a case.¹⁹³ He concluded that the Internet infrastructure service providers could be divided into three major categories: Internet content provider (ICP), Internet service provider (ISP), and Internet apparatus provider (IAP). ICPs select, edit, and upload information content; ISPs facilitate the transmission of information without selecting or editing the contents; and IAPs provide essential apparatuses for network operation. Since case law is not bound in China, the definition of ISP within the case law is merely a reference for the Chinese legislature.

¹⁹³ Music Copyright Society of China (MCSC) v. Guangzhou NetEase Inc. and China Mobile Beijing Ltd. Beijing Second Intermediate People's Court (2002) Er Zhong Min Chu Zi No. 03119.

To import a new definition into the Chinese legal regime, the People's Supreme Court could provide a judicial interpretation in the Provision about the definition of ISP. Later, the Chinese legislature could consider enacting the definition in Chinese law if such a definition is accepted by the public. Since China is a member of WCT, the definition of ISP in China should comply with Article 8 of WCT. Moreover, technology develops very fast, the definition of ISP should also be broad enough to cover the current three major categories of ISPs and potential categories of ISPs in the future. Otherwise, the new ISP model may not be able to cover new categories of ISPs. For example, in *Aereo*, the Aereo company provided an online retransmit service by a physical antenna. The antenna captures and transcodes over-the-air broadcast television programming signals. Although Aereo's server retransmits the programming by Cloud technology, copyright programming is stored on its subscribers' personal electric device. According to the aforementioned ISP definition, Aereo fits all three categories. Consequently, such a flawed ISP definition may cause legal uncertainty. In the future, new categories of ISPs may emerge by new technologies or business models. Therefore, the new definition of ISP should be broad to adapt to new technological environments.

Both China and Japan are civil law countries. Since the ISP definition from Japan is broad, the Chinese legislature could consider legally transplanting the Japanese ISP definition. Professor Luo Yong from Chongqing University suggested that the Chinese legislature should take the ISP definition from Japan in Article 2 (iii) of Limitation of Provider liability Act into consideration.¹⁹⁴ A practical way for China to adopt a new definition of ISP is that the Supreme People's Court could legally transplant Japanese ISP definition into the Provision first. If the new definition is accepted by the public, the Chinese legislature could amend it into RCI Regulation in the future.

¹⁹⁴ Luo, *supra* note 18, at 99.

2. Legal conflict

Shifting away from a passive-reactive ISP model toward an active-preventive ISP model may cause legal conflict with current law. So far the traditional passive-reactive ISP statutes still exist in most of the countries,¹⁹⁵ including China and the U.S. The active-preventive ISP principles may cause controversial issues in ISP-related regulations. For example, in *YouTube*, the Second Circuit applied something more standard that required the ISP to “institute a monitoring program.”¹⁹⁶ However, the DMCA Section 512(m) prohibits an ISP from monitoring its service and illegal access to the material on its network.¹⁹⁷ The same controversial issues can be found in China. As mentioned in Chapter III, the paradox in *Baidu* is that the Provision requires ISPs “proactively take[] reasonable measures to prevent infringement,”¹⁹⁸ while ISPs do not have to “conduct proactive examination regarding to network user’s infringement . . .”¹⁹⁹ As a result, the Provision does not provide what exactly an ISP should do or should not do in order to prevent copyright infringement. The next Chapter discusses how to solve this uncertainty in Chinese copyright regimes.

¹⁹⁵ JEREMY & CHRISTOPHER, *supra* note 32, at 377-378.

¹⁹⁶ *Viacom*, 676 F.3d at 38.

¹⁹⁷ 17 U.S.C. § 512(m).

¹⁹⁸ The Provision, art. 9 (iv)

¹⁹⁹ The Provision, art. 8 para. 2.

Chapter VI.

Alternative solutions

This Chapter examines what an ISP should do to actively prevent copyright infringement and provides several solutions from both legal and technical perspectives. On the legal perspective, this chapter introduces the graduated response, which has been a controversial ISP policy over the world. On the technical perspective, this chapter borrows the piracy experience from the video game industry and introduces a new technical solution: Denuvo anti-tamper technology.

A. “Standard technical measure” exception

1. Section 512 (i)

In the U.S., the something more standard requires an ISP to “institute a monitoring program,”²⁰⁰ while the DMCA Section 512(m) prohibits an ISP from monitoring its service.²⁰¹ The issue is what an ISP should do in order to fulfill something more standard requirement. The DMCA Section 512 (m) provides a standard technical measure exception for ISP to monitor its network.²⁰² Section 512 (i)(2)(A) defines a standard technical measure as “an open, fair, voluntary, multi-industry standard process.”²⁰³ In addition, a standard technical measure should have reasonable availability and cost.²⁰⁴ In *YouTube*, the Second Circuit did not discuss the relationship between the something more standard and standard technical measure exception. According to the discussion of the something more standard,

²⁰⁰ *Viacom*, 676 F.3d at 38.

²⁰¹ 17 U.S.C. § 512(m).

²⁰² 17 U.S.C. § 512(m)(1).

²⁰³ 17 U.S.C. § 512(i)(2)(A).

²⁰⁴ 17 U.S.C. § 512(i)(2)(B)-(C).

the Second Circuit may indicate that ISPs should actively adopt standard technical measure to prevent copyright infringement.

2. Reasonable duty of care

Similar statutes like Section 512(i) can be found in China. In addition to Article 9 (iv) of the Provision, Article 8 paragraph 3 of the Provision provides an exception for ISP if an ISP “has taken reasonable and effective technical measures.”²⁰⁵ But the Provision does not provide specific definition about the technical measure. According to the requirements from the Provision, the Supreme People’s Court may indicate that an ISP should actively develop and adopt reasonable and effective technical measures to prevent copyright infringement on its network. However, an appropriate technical measure for ISP may vary from the technological innovation and the ISP policy. The next section further discusses a controversial active-preventive solution: the graduated response, which is an interesting attempt to solve the ISP issues. The rest of this chapter also introduces a possible technical measure for ISP solution: Denuvo anti-tamper technology.

B. The Graduated Response

1. Historical context

The graduated response procedure was known as “three strikes and you are out” that originated from a baseball rule. Some scholars describe the graduated response procedure as “digital guillotine,”²⁰⁶ which reflects how it terminates people’s Internet connection. In the

²⁰⁵ The Provision art. 8 para. 3: Where a network service provider is able to prove that it has taken reasonable and effective technical measures but it is still difficult for it to discover a network user's infringement of the right of dissemination on information networks, the court shall determine that the network service provider is not at fault.

²⁰⁶ WILLIAM PATRY, MORAL PANICS AND THE COPYRIGHT WARS 14 (2009).

European Union (EU), The graduated response is also called “Three Strikes disconnection policies”²⁰⁷. The general three strikes policy works similarly to the EU policy:

After identifying Internet users alleged to be engaged in copyright violation by collecting their Internet Protocol addresses (IP addresses), copyright holders would send the IP addresses of those users to the relevant Internet service provider(s) who would warn the subscriber to whom the IP address belongs about his potential engagement in copyright infringement. Being warned by the ISP a certain number of times would automatically result in the ISP's termination or suspension of the subscriber's Internet connection.

In May 2009, France passed its graduated response law named Law Promoting the Distribution and Protection of Creative Works on the Internet (Creation and Internet Act), which established a new administrative authority, the High Authority for the Dissemination of Works and the Protection of Rights on the Internet (HADOPI) to impose its graduated response policy. The Creation and Internet Act entered into effect on January 1, 2010.²⁰⁸ So far, the graduated response law exists in some countries, but in the past have not been norm.²⁰⁹

The graduated response procedure benefits copyright owners because it helps prevent repeated copyright infringements. By cooperating with copyright owners, ISPs also benefit from the graduated response procedure because it can prevent ISPs from secondary copyright liabilities. However, the Internet users may complain about the graduated response procedure after receiving warnings from ISP because they are concerned about being disconnected from the Internet.²¹⁰ The next section examines the benefits and drawbacks of the graduated

²⁰⁷ Opinion of the European Data Protection Supervisor on the current negotiations by the European Union of an Anti-Counterfeiting Trade Agreement (ACTA), paragraph 21 & 22.
https://secure.edps.europa.eu/EDPSWEB/webdav/shared/Documents/Consultation/Opinions/2010/10-02-22_AC TA_EN.pdf (last visited Oct 25, 2016).

²⁰⁸ LOI no 2009-669 du 12 juin 2009 favorisant la diffusion et la protection de la création sur internet (Law No. 2009-669 of June 12, 2009 to Promote the Dissemination and Protection of Creation on the Internet), Journal Officiel de la République Française [J.O.] [Official Gazette of France], June 12, 2009, p. 9666, available at [http://legifrance.gouv.fr/affichTexte.do?sessionId=69C25044 ICO4AFAED3A3EC46276A39BD.tpdjo l4v1 ?cidTexte=JORFTEXT000020735432&categorieLien=id](http://legifrance.gouv.fr/affichTexte.do?sessionId=69C25044 ICO4AFAED3A3EC46276A39BD.tpdjo l4v1 ?cidTexte=JORFTEXT000020735432&categorieLien=id.). "HADOPI" stands for the 'High Authority for the Diffusion of Works ('Oeuvres' in French) and the Protection of Rights on the Internet."

²⁰⁹ JEREMY & CHRISTOPHER, *supra* note 32, at 388.

²¹⁰ HUA, *supra* note 21, at 123.

response procedure, and discusses whether China should adopt this policy. Due to the scope and length of this chapter, the analysis mainly focuses on the ISP side.

2. ISP

a. Benefits

First, the graduated response system can help the ISPs avoid the constant need to respond to lawsuits and the high costs of legal defense,²¹¹ which is exactly a cure for Baidu issue in China. As mentioned in Chapter I, from 2011 to 2014, copyright owners over the world brought lawsuits against Baidu more than 40 times.²¹² By adopting the graduated response system, ISPs may not be held directly or indirectly liable for the infringing activities of Internet users. No matter whether the Chinese legislature would adopt the graduated response system into Chinese law, Baidu should definitely adopt it to avoid being scapegoats for their users' infringing activities.²¹³ Consequently, Baidu can spend more resources on developing and improving its network services instead of handling lawsuits.

Second, the graduated response system may facilitate the cooperation between ISPs and copyright owners.²¹⁴ As mentioned above, Baidu has a tense relationship with copyright owners, and most of the copyright owners consider Baidu a disaster in copyright protection regimes. The graduated response provides an alternative mechanism to fight Internet piracy. It goes beyond a traditional passive-reactive approach and implies an educational notification mechanism for alleged online infringers before more stringent measures can be imposed.²¹⁵ In *Baidu*, the Beijing High People's Court held that the ISP should actively try to contact the

²¹¹ See Alfred C. Yen, *Internet Service Provider Liability for Subscriber Copyright Infringement, Enterprise Liability, and the First Amendment*, 88 GEO. L.J. 1833, 1887-88 (2000).

²¹² Zhang, *supra* note 3, at 29.

²¹³ Peter K. Yu, *The Graduated Response*, 62 FLA. L. REV. 1373, 1384 (2010).

²¹⁴ *Id.*

²¹⁵ See Alain Strowel, *Internet Piracy as a Wake-up Call for Copyright Law Makers-Is the "Graduated Response" a Good Reply?*, 1 WIPO J. 75, at 77 (2009).

uploader, verify the related documents and adopt effective measures to prevent infringement.²¹⁶ Therefore, adopting the graduated response may ease the relationship between Baidu and copyright owners. Moreover, by following the court's decision, Baidu may be able to building a more active-preventive ISP model in China.

Third, as Professor Strowel elaborated, the graduated response system has educative and rehabilitative benefits.²¹⁷ In *Baidu*, the number of hits of the infringing document was more than 200,000.²¹⁸ As a consequence of the previous absence of strong governmental execution and general education on copyright law, a culture that respects copyright has not been established in China yet.²¹⁹ Adopting the graduated response may be an effective and public acceptable way of copyright education for Chinese society.

b. Drawbacks

The major drawback of the graduated response system is that it is costly to ISP by raising the costs of surveillance, policing, and data retention. Such financial burden may cause ISP to stop improving their network or offering low-cost services.²²⁰ The financial problem is fatal for any small ISP companies, but it might not be a problem for the second-largest search engine company Baidu.²²¹ To prevent copyright infringement, Baidu established "Green Channels for Copyright Infringement Report" in "Wenku Report Center" in March 2011. The copyright owners can report the infringing materials on Baidu Wenku so that the employees of Baidu would expeditiously remove or block the infringing materials.²²² Ironically, In September 2011, Baidu closed the literature section in Baidu Wenku due to the

²¹⁶ *Baidu Wenku*, at 25, Beijing High People's Ct. Aug 5, 2014.

²¹⁷ Strowel, *supra* note 215, at 86.

²¹⁸ *Id.* at 2.

²¹⁹ HUA, *supra* note 21, 129.

²²⁰ Yu, *supra* note 213, 1391-1392.

²²¹ EMARKETER, *supra* note 91.

²²² *Baidu Wenku*, at 16, Beijing High People's Ct. Aug 5, 2014.

huge amount of piracy.²²³ Therefore, the financial burden is not a primary issue for Baidu, otherwise Baidu would not invest its “Green Channel” project and manually censor the uploading documents that are more than one thousand Chinese words.²²⁴ Moreover, the financial burden is not the reason why Baidu closed the literature section in Baidu Wenku, which is free for the public. Overwhelmed piracy documents forced Baidu to close its free online service. In sum, Baidu needs an effective and publicly accepted policy to fight against online piracy. Therefore, financial drawback of the graduated response procedure is not an issue for solving Baidu issue.

Although the graduated response procedure might be a solution for Baidu issue in China, the Chinese legislature should be prudent on legally transplanting this policy because a new graduated response law may bring an adverse effect to Internet users in China. As mentioned before, copyright is a serious issue in China. Many Internet users in China do not even know or even care about copyright. Applying graduated response procedure may cause millions of people to disconnect from the Internet. Noted author William Patry suggested that “[t]he term graduated response should be replaced with the more accurate term 'digital guillotine,' reflecting its killing of a critical way people connect with the world and in some cases, eliminating their ability to make a living.”²²⁵ Therefore, it is too controversial for Chinese legislature to enact it into Chinese law. However, Baidu, as an ISP in China that was overwhelmed by copyright infringement, should consider adopting the graduated response procedure in its copyright protection policy. The next question is that how a Chinese ISP adopts and enforces the graduated response procedure. The ISP in the U.S. provides sufficient experience for Chinese ISP to learn.

²²³ *Id.* at 2-3.

²²⁴ *Id.* at 13.

²²⁵ PATRY, *supra* note 206, at 14.

3. The Graduated Response procedure from the U.S.

The U.S. did not adopt graduated response law. However, in order to avoid indirect copyright liability, some ISPs in the U.S. adopted the graduated response procedure. For example, Indiana University (IU) adopted it in its online safety & security policy.²²⁶ As an ISP, IU provides its own wireless network “IU Secure” for all the students and faculties. IU does not actively monitor its network. However, if IU receives a notice-and-takedown notification from the copyright owner, the IT department of IU would disable the infringer’s access to IU wireless network immediately, and the University Information Policy Office would send a first violation email to the infringer, including fine and a copy of the complaint from the copyright holder. The infringer is required to complete the tutorial and quiz in order to regain the access to IU wireless network.²²⁷ If the infringing activity occurs three times, in addition to an expensive fine, infringer’s access to the IU network is blocked permanently. Although the repeated infringer could still access the Internet in other ways, the ISP has actively punished the infringer and prevented the infringement activities.

As a conclusion, adopting graduated response procedure may effectively punish the infringer and prevent the infringement activities. The graduated response procedure is optional for China to adopt because it is still controversial and not all ISPs are suitable for graduated response procedures. However, by adopting the graduated response procedures, ISP that is overwhelmed by copyright infringements, such as Baidu, may obtain significant effect on copyright protection. The ISP in the U.S., such as IU, provides sufficient detail on how to adopt graduated response procedures to prevent copyright infringement. Not only should Chinese ISPs consider adopting the graduated response procedure, the IU graduated

²²⁶ *Copyright tutorial IU*, <https://protect.iu.edu/online-safety/personal-preparedness/file-sharing/tutorial.html> (last visited Oct. 25, 2016).

²²⁷ *Copyright infringement incident resolution IU*, <https://protect.iu.edu/online-safety/personal-preparedness/file-sharing/violations.html> (last visited Oct. 25, 2016).

response system is also a reference for Chinese executive department. In the executive branch, the National Copyright Administration (NCA) or the Ministry of Information Industry (MII) can enact the graduated response into administrative regulation, such as ICM, to enforce adopting the graduated response procedures on Chinese ISPs by executive orders.

C. A technical solution

Although the graduated response procedure might be a legal solution for Baidu issue, new technology is another way to solve this issue. As mentioned in *Baidu*, the fingerprint system is not able to prevent copyright infringement. The question is which technology is the standard technical measure for ISPs to protect copyright on their networks? Since the technology developed so fast, the answer may vary from time to time. The fingerprint system may be a standard technical measure five years ago, but now it has been so easy to be circumvented. This section does not go further into the legal discussion about technological protection measures (TPMs),²²⁸ and only suggests a technical proposal for ISPs to think about.

The fatal weakness of TPMs is: hacker can defeat each new TPMs within a short time. For example, video game companies were suffered by circumvents measures for decades. Hackers were able to defeat its digital rights management (DRM) scheme almost as soon as the game was released. Usually within one to two weeks, the DRM of games will be cracked. However, this situation has been changed since the Austrian Denuvo Software Solutions GmbH invented its anti-tamper technology: Denuvo.

Denuvo is not a DRM solution; it protects the DRM solutions from being

²²⁸ See WCT art. 11. See also 17 U.S.C. § 1201(a)-(b).

circumvented.²²⁹ An early report even suggested that Denuvo “continuously encrypts and decrypts itself so that it is impossible to crack.”²³⁰ The working mechanism of this technology is not the point in this section. The main concern is that how does it works for copyright protection? Usually, a new version of a game releases every year, and the first month sale is really important for Video Game Company. According to Denuvo’s report, one of the latest Denuvo-protected games has gone without being cracked for more than 270 days.²³¹ Besides video games, Denuvo’s technology can also apply on eBooks, software, video and media quality control. It allows only a legitimate user account to use the digital files or software. Consequently, a simply application of this technology may prevent most of the copyright infringement through an ISP network. Even though an infringer downloads a digital material from the Internet, the material is under the protection of Denuvo.

Although Denuvo can provide a better protection for digital copyright work, two common drawbacks of TPMs still exist in this new technology. First, financial cost of this technology could be unaffordable to small ISP companies. Second, all TPMs may eventually be cracked by hackers; it is just a matter of time. As a conclusion, a perfect technology for copyright protection does not exist. As Professor Strowel elaborated: “[A] solution that would eliminate all piracy, if at all possible, would seem dangerous or at least dubious for both individual liberties and technological innovation.”²³²

Although no technology is perfect for copyright protection, new technology can do a better job than old one. Thus, embracing the new technology for a better copyright protection would be a good strategy for ISP. Both Copyright owners and ISPs could actively cooperate with new-tech company to accomplish a better protection. As aforementioned, law is always

²²⁹ *What is the Denuvo Anti-Tamper solution?* DENUVO, <http://www.denuvo.com/> (last visited Oct. 27, 2016).

²³⁰ Karan Kalra, *How The New DRM Denuvo Might Be Damaging Your SSD* [Update] (Nov. 18, 2014), <https://web.archive.org/web/20150119041502/http://asidcast.com/index.php/2014/11/new-drm-denuvo-might-damaging-ssd> (last visited Oct 27, 2016).

²³¹ *What do we do?* DENUVO, <http://www.denuvo.com/> (last visited Oct .27, 2016).

²³² Strowel, *supra* note 215, at 86.

slower than technological development. The graduated response procedure maybe a good copyright protection policy for an active-preventive ISP model, but it takes time for legislature to enact a policy into law. On the contrary, new technology is available to protect copyright as long as a third party decides to use it. As a big tech-company, Baidu should consider upgrading its TPMs from fingerprint system to new technology. Denuvo would be a good option.

Chapter VII

Conclusion

As aforementioned in *YouTube* and *Baidu*, the current international trend is shifting from a passive-reactive ISP model to an active-preventive model. Although the Japanese Supreme Court still maintains a traditional passive-reactive ISP approach, courts in China and the U.S. have followed this trend in their own way. In the U.S., the court applied something more standard that required the ISP to exert substantial influence on the activities of Internet users. In China, the court requires the ISP to pay reasonable duty of care on its network. The comparative study of these legal theories and cases show that the Chinese legislature should follow an active-preventive ISP model to solve the copyright infringement issues of ISPs, such as Baidu. As a proposal for China to solve the Baidu issue, this thesis suggests that Baidu could adopt the graduated response procedure to prevent its users from copyright infringement. Also, Baidu could think about cooperating with copyright owners to adopt new technology to prevent copyright infringement, such as the Denuvo anti-tamper technology.

This thesis does not attempt to degrade the passive-reactive ISP model. It might still work very well in certain situations, such as national circumstance in Japan. However, a traditional passive-reactive ISP model has been proved unsuccessful in China. As aforementioned in Chapter I, Baidu has been sued multiple times by different copyright owners over the world, but copyright owner could do nothing to prevent Baidu from copyright infringement. To solve the ISP issue like Baidu, this thesis suggests a proposal of an active-preventive ISP legal reform in China and recommends that the copyright owner and ISPs in China think about the application of new technology.

Legal solutions for the ISP issues are limited because ISP-related law is always slower than technological innovation, but the power of the new technology is unpredictable. Therefore, not only should legal scholars and lawmakers focus on ISP policy, but also pay attention to applying new technology to ISP model, which may provide a better legal solution for ISP issues in the future. The Chinese government should absolutely lead the way to further the reform of an active-preventive ISP model. Moreover, for the best interest of Baidu, it should also consider following the active-preventive trend by adopting new policy and technology.

Reference

Books

- CRAIG JOYCE ET AL., COPYRIGHT LAW (LexisNexis. 9th ed. 2013).
- ROGER E. SCHECHTER & JOHN R. THOMAS, INTELLECTUAL PROPERTY: THE LAW OF COPYRIGHTS, PATENTS AND TRADEMARKS (West 2003).
- ROCHELLE C. DREYFUSS & ROBETRA R. KWALL, INTELLECTUAL PROPERTY: CASES AND MATERIALS ON TRADEMARK, COPYRIGHT, AND PATENT LAW (Foundation Press. 2d ed. 2004).
- PAUL GOLDSTEIN & MARKETA TRIMBLE, INTERNATIONAL INTELLECTUAL PROPERTY LAW CASES AND MATERIALS (Foundation Press, 4th ed. 2016).
- SONG, SEAGULL HAIYAN, NEW CHALLENGES OF CHINESE COPYRIGHT LAW IN THE DIGITAL AGE (Wolters Kluwer 2011).
- JERRY JIE HUA, TOWARD A MORE BALANCED APPROACH: RETHINKING AND READJUSTING COPYRIGHT SYSTEM IN THE DIGITAL NETWORK ERA (Springer 2014).
- MARSHALL A. LEAFFER, UNDERSTANDING COPYRIGHT LAW (LexisNexis 5th ed. 2010).
- WILLIAM PATRY, MORAL PANICS AND THE COPYRIGHT WARS (2009)

Periodical Materials

- Alain Strowel, *Internet Piracy as a Wake-up Call for Copyright Law Makers-Is the "Graduated Response" a Good Reply?*, 1 WIPO J. 75 (2009)
- Alfred C. Yen, *Internet Service Provider Liability for Subscriber Copyright Infringement, Enterprise Liability, and the First Amendment*, 88 GEO. L.J. 1833 (2000)

- Jeremy de Beer & Christopher D. Clemmer, *Global Trends in Online Copyright Enforcement: A Non-Neutral Role for Network Intermediaries?*, 49 JURIMETRICS J. 375 (2009).
- Zhang Yanhong (张艳红), *China Youth Publishing Group sue Baidu and win on the court of first instance* (中国青年文库诉百度一审胜诉), *Electronics Intellectual Property* (电子知识产权), Z1-2015.
- Luo Yong (罗勇), *Legal definition about “network service provider”*(论“网络服务提供者”的法律界定), *Academic Exchange* (学术交流) Serial No. 267, No. 6, Jun, 2016.
- Ji Chendi (姬晨笛), *Research on the Legal Nature of China's "Safe Haven" Rule* (我国“避风港”规则的法律性质研究), *Electronics Intellectual Property* (电子知识产权), Z1-2016.
- Jiang Bo (江波) & Zhang Jinping (张金平), *Research on the ISP's knowledge standard – rethink “red flag provision”* (网络服务提供者的知道标准判断问题研究——重新认识“红旗标准”), *Journal of law application* (法律适用), No. 12, 2009, at 55.
- Ridwan Khan, *Pure Software in an Impure World? WINNY, Japan's First P2P Case* 8 E. ASIA L. REV. 21, 24 (2013)
- Peter K. Yu, *The Graduated Response*, 62 FLA. L. REV. 1373 (2010)

Cases

- *American Broadcasting Crop. v. Aereo*, 134 S.Ct. 2498 (2014)
- Běijīng zhōng qīng wén wénhuà chuánméi yǒuxiàn gōngsī děng zhùzuòquán quán shǔ, qīnquán jiūfēn èrshěn mínshì pàn jué shū (北京中青文文化传媒有限公司等著作权

- 权属、侵权纠纷二审民事判决书) [China Youth Publishing Group v. Baidu Wenku], 2014 Gao Min Zhong Zi No. 2045 (Beijing High People's Ct. Aug 5, 2014)
- Music Copyright Society of China (MCSC) v. Guangzhou NetEase Inc. and China Mobile Beijing Ltd. Beijing Second Intermediate People's Court (2002) Er Zhong Min Chu Zi No. 03119.
 - Saika Saibansho [Sup. Ct.] Dec. 19, 2011, 2009 (A) No. 1900, 65 SAIKO SAIBANSHO KEIJI HANREISHU [KEISHU]
 - *Viacom Int'l, Inc. v. YouTube, Inc.*, 718 F. Supp. 2d 514 (S.D.N.Y. 2010)
 - *Viacom Int'l, Inc. v. YouTube, Inc.*, 676 F.3d 19 (2d Cir. 2012)
 - *UMG Recordings, Inc. v. Shelter Capital Partners LLC*, 718 F.3d 1006 (9th Cir. 2013)
 - *Sony Corp. of America v. Universal City Studios, Inc.*, 104 S.Ct. 774, 785 (1984)
 - *Fonovisa, Inc. v. Cherry Auction, Inc.*, 76 F.3d 259 (9th Cir. 1996)
 - *Parker v. Google, Inc.*, 242 Fed.Appx. 833 (3d Cir.2007)
 - *Gershwin Publishing Corp. v. Columbia Artists Management, Inc.*, 443 F.2d 1159 (2d Cir.1971)
 - *Metro-Goldwyn-Mayer Studios Inc. v. Grokster, Ltd.* 125 S. Ct. 2764 (2005)

Statutes

- 17 U.S.C.§101 (2010)
- 17 U.S.C.§106 (2002)
- WIPO Copyright Treaty Art 8.
- Digital Millennium Copyright Act, 17 U.S.C.§512 (2010)
- Chosakkun Ho [Copyright Act] Act No. 39 of 1899 (Japan)
- Chosakkun Ho [Copyright Act] Act No. 48 of 1970 (Japan)
- Chosakkun Ho [Copyright Act] Act No. 73 of 2009 (Japan)

- Kei Hou [Penal Code] Act No. 54 of 2007 (Japan)
- Minji soshō-hō [Code of Civil Procedure] Act No.36 of 2011 (Japan)
- Tokutei denki tsūshin ekimu teikyō-sha no songai baishō sekinin no seigen oyobi hasshinsha jōhō no kaiji ni kansuru hōritsu [Purobaida sekinin seigen-hō] [Act on the Limitation of Liability for Damages of Specified Telecommunications Service Providers and the Right to Demand Disclosure of Identification Information of the Senders (Limitation of Provider liability Act)] Act No. 137 of 2001 (Japan).
- Xin xi wang luo chuan bo quan bao hu tiao li (信息网络传播权保护条例) [Regulations for the Protection of the Right of Communication through Information Network] (promulgated by the St. Council, May 18, 2006, amended by the St. Council in Jan 30, 2013) (China).
- Zhong hua ren min gong he guo zhu zuo quan fa (中华人民共和国著作权法) [Copyright Law of the PRC] (promulgated by the Standing Comm. Nat'l People's Cong., Sep. 7, 1990, second amended by the Standing Comm. Nat'l People's Cong., Feb. 26. 2010)
- Hu lian wang zhu zuo quan xing zheng bao hu ban fa (互联网著作权行政保护办法) [Measures for the Administrative Protection of Internet Copyright Measures] (promulgated by NCA & MII, Apr. 29, 2005, effective May 1, 2005), art 5, translated by Bei da fa bao (en.pkulaw.cn).
- Zhong hua ren min gong he guo qing quan ze ren fa (中华人民共和国侵权责任法) [Tort Law of the PRC] (promulgated by the Standing Comm. Nat'l People's Cong., Dec. 26, 2009, effective in Jul. 1, 2010)
- Zui gao ren min fa yuan guan yu sheng li qing hai xin xi wang luo chuan bo quan min shi jiu fen an jian shi yong fa lv ruo gan wen ti de gui ding(最高人民法院关于审理

侵害信息网络传播权民事纠纷案件适用法律若干问题的规定) [Provisions of the Supreme People's Court on Several Issues concerning the Application of Law in Hearing Civil Dispute Cases Involving Infringement of the Right of Dissemination on Information Networks] (promulgated by the Sup. People's Ct., Dec. 12, 2012, effective Jan. 1, 2013) Interpretation No. 20 [2012] of the Sup. People's Ct. translated by Bei da fa bao (en.pkulaw.cn).

- Zhōnghuá rénmin gònghéguó rénmin fǎyuàn zǔzhī fǎ (中华人民共和国人民法院组织法) [Organic Law of the People's Courts of the People's Republic of China] (promulgated by the St. Council, Jul 1, 1979, amended by the St. Council in Oct 31, 2006) (China).
- LOI no 2009-669 du 12 juin 2009 favorisant la diffusion et la protection de la création sur internet (Law No. 2009-669 of June 12, 2009 to Promote the Dissemination and Protection of Creation on the Internet), Journal Officiel de la République Française [J.O.] [Official Gazette of France], June 12, 2009, p. 9666, (France)

Internet Materials

- Copyright tutorial, <https://protect.iu.edu/online-safety/personal-preparedness/file-sharing/tutorial.html> (last visited Oct. 25, 2016).
- Copyright infringement incident resolution, <https://protect.iu.edu/online-safety/personal-preparedness/file-sharing/violations.html> (last visited Oct. 25, 2016).
- NETFLIX, *How does Netflix work?* <https://help.netflix.com/en/node/412?lang=en&nodeId=412> (last visited Aug. 27, 2016)

- Miguel Helft & Michael Wines, *Google Faces Fallout as China Reacts to Site Shift* (Mar. 23, 2010), http://www.nytimes.com/2010/03/24/technology/24google.html?pagewanted=1&_r=0&hp (last visited Oct. 7, 2016)
- EMARKETER, *Google Will Take 55% of Search Ad Dollars Globally in 2015*, <http://www.emarketer.com/Article/Google-Will-Take-55-of-Search-Ad-Dollars-Globally-2015/1012294> (last visited Nov. 3, 2016)
- 37th Statistical Report on Internet Development in China, http://cnnic.cn/hlwfzyj/hlwzxbg/hlwtjbg/201601/t20160122_53271.htm (last visited Sep. 8, 2016). English version is available at <http://cnnic.com.cn/IDR/ReportDownloads/>
- Heisei 21-nen chosakukenhō kaisei no pointo (Points on 2009 Copyright Act Amendment) <http://dan-law.jp/commentary/H21Copyright-Commentary.pdf> (last visited Oct. 2, 2016)
- Opinion of the European Data Protection Supervisor on the current negotiations by the European Union of an Anti-Counterfeiting Trade Agreement (ACTA), paragraph 21 & 22. https://secure.edps.europa.eu/EDPSWEB/webdav/shared/Documents/Consultation/Opinions/2010/10-02-22_ACTA_EN.pdf, (last visited Oct 25, 2016).
- Karan Kalra, *How The New DRM Denuvo Might Be Damaging Your SSD* [Update] (Nov. 18, 2014) <https://web.archive.org/web/20150119041502/http://asidcast.com/index.php/2014/11/new-drm-denuvo-might-damaging-ssd> (last visited Oct. 27, 2016).
- DENUVO, *What is the Denuvo Anti-Tamper solution?*, <http://www.denuvo.com/> (last visited Oct. 27, 2016)

- DENUVO, *What do we do?*, <http://www.denuvo.com/> (last visited Oct. 27, 2016)

Others

- Hsin-an Yao, *New advances in ISP's copyright liability in China and Taiwan* (Dec. 2006) (unpublished L.L.M. thesis, Indiana University) (on file with Indiana University library system).