2019

Evaluating a Unified Intellectual Property System of Internet Service Providers in the Electronic Commerce Law -- A Comparative Research Between China and the U.S.

Yifan Huang
Indiana University Maurer School of Law, rafael.huang@hotmail.com

EVALUATING A UNIFIED INTELLECTUAL PROPERTY SYSTEM OF INTERNET SERVICE PROVIDERS IN THE ELECTRONIC COMMERCE LAW - A COMPARATIVE RESEARCH BETWEEN CHINA AND THE U.S.

YIFAN HUANG

Submitted to the faculty of Indiana University Maurer School of Law

in partial fulfillment of the requirements

for the degree

Doctor of Juridical Science

MAY 2019

Accepted by the faculty, Indiana University Maurer School of Law, in partial fulfillment of the requirements for the degree of Doctor of Juridical Science.

Doctoral Committee

Marshall Leaffer (Chairman)

Mark Janis

Michael Mattioli

April 4th, 2019.

ACKNOWLEDGMENT

Four years ago, I started my LLM degree in a lovely town, Bloomington. At that time, I would never expect to spend the next four years to accomplish my SJD degree. On the way of writing my dissertation, I could not have finished it without the guidance and support of many people, including my family, friends and colleagues.

First, I have to express my sincere gratitude to my supervisor, Professor Marshall A. Leaffer, for being a great mentor and advisor. I would never stay in Maurer School of Law to start my SJD without his supervision on my LLM Thesis. 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.

The same gratitude must be also given to my committee, Prof. Mark Janis and Prof. Michael Mattioli, who helped me at the final stage of my writing and provided me lots of insightful comments on my manuscript. Without your help, it might take me more time to finish my dissertation qualified for final defense.

My special thanks go to Dean Lesley Davis who supported me to be a student ambassador, and Prof. Goodwin who supervised me when I worked as a co-coordinator for the Graduate Colloquium.

Finally, 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.

ABSTRACT

As the Electronic Commerce Law went into effective in Jan. 1st, 2019, not only did China establish a unified IP protection system of ISPs, but also set up a blueprint for a comprehensive mechanism of ISPs for the future improvement. The question is whether this new law can effectively prevent the serious IP infringement issues of ISPs and therefore successfully improve the IP protection in China. To answerer this question, the dissertation analyzes the development of the mechanism of ISPs in copyright and trademark regimes before the Electronic Commerce Law, and seeks to demonstrate the impact of the Electronic Commerce Law for ISPs in China through a comparatively research.

Before the Electronic Commerce Law, China followed a passive-reactive approach of ISPs from the U.S. However, as the online piracy and counterfeit issues continued to grow in the last decade, Chinese legislation decided to shift to an active-preventive approach of ISPs in the Electronic Commerce Law. By comparatively examining the copyright and trademark infringement issues of ISPs between China and the U.S., this dissertation analyzes the benefits and drawbacks of these two approaches, and seeks to demonstrate how an active-preventive approach may prevent infringements more effectively than a passive-reactive approach in China.

To conclude a solution for Chinese legislation to improve the unified IP protection system of ISPs, this dissertation examines several active-preventive approaches in different jurisdictions through different cases of ISPs. As a suggestion for the future legal reform, this dissertation explores the possibility of whether Chinese legislation can legally transplant the Blocking Injunction into the unified IP protection

system of ISPs, which may improve the mechanism of ISPs and provide a better IP protection in China.

TABLE OF CONTENT

Chapter I: Introduction

A. Background

1. Global Intellectual Property Issues

After the economy crisis from 2011 to 2013, Intellectual Property Right (IPR) related industries have become a new engine of the global economy growth. The G7 ICT[1] and Industry Minister's Declaration 2017 (hereinafter "G7 Declaration") acknowledged "…the role of intellectual property rights for promoting innovation, contributing to industry's productivity, growth and competitiveness in the digital economy and that IPR-intensive industries contribute more than other industries to increase GDP, employment and trade."[2] In short, IPRs play important roles on global economy in digital age. For example, in the European Union (EU), IPR-intensive industries contributed 86% of imports and 93% of exports to EU external trades, and 42% of GDP.[3] Nonetheless, the growth of IPR-intensive industries come with the rise of IP infringements in the digital economy.

IP infringement affects legitimate economies, causing potential harm to citizens and IP business, especially contributing to reduced revenues for the affected businesses, decreased sales volume and job losses.[4] For example, in 2013, "IPR-infringing products now originate from virtually all geographical areas and economies globally, constituting up to 2.5 % of all global trade, worth up to USD 461 billion."[5] The main reason of this IP infringement issue is

---

[1] Information and Communications Technology.
[2] G7 ICT and Industry Ministers' Declaration, Torino, Italy (September 25-26, 2017), at 13-14. http://www.g7italy.it/sites/default/files/documents/G7%20ICT_Industry_Ministers_Declaration_%20Italy-26%20Sept_2017final_0.pdf
[3] European Patent Office and the European Union Intellectual Property Office, Intellectual property rights intensive industries and economic performance in the European Union, 2016, at 6. Available at: https://euipo.europa.eu/tunnel-web/secure/webdav/guest/document_library/observatory/documents/IPContributionStudy/performance_in_the_European_Union/performance_in_the_European_Union_full.pdf.
[4] 2017 Situation Report on Counterfeiting and Piracy in the European Union, at 3.
[5] OECD/EUIPO (2016), Trade in counterfeit and pirated goods mapping the economic impact, 2016, at 11. Available at: http://www.oecd.org/gov/risk/trade-in-counterfeit-and-pirated-goods-9789264252653-en.htm.

that there is no harmonized IP enforcement mechanism in the world. As the G7 Declaration recognized: "… the need to have in place strong enforcement mechanisms for IP, including through international collaboration, to the benefit of IP right holders engaged in both large and small businesses, in light of serious risk of economic loss stemming from IP infringement including counterfeiting, piracy and misappropriation of trade secrets."[6] As a result, building up strong IP enforcement mechanisms for better IP protections is critical to the overall growth of economy in the world.

2. IP Issues in China

For the purpose of building up IP enforcement mechanisms through international collaboration, inevitably, the protection of IPRs in China (i.e. PRC)[7] is the crux. The main reason why China is important for global IP protection is because it has been recognized as the engine of the global counterfeiting industry.[8] Counterfeit goods are estimated to amount to approximately 12.5 % of China's total exports and over 1.5 % of its GDP. This results in estimations that 72 % of counterfeit goods currently in circulation in three of the world's largest markets for such products, namely the EU, Japan and the USA, were exported from China.[9] As a result, it is impossible to build strong global IP enforcement mechanisms without solving IP infringement issues in China.

Not only did the IP infringement issues in China harm the global economy, but it also encumbered the healthy development of Chinese economy and IP industry. In 2016, Chinese administrative law enforcement authorities investigated and processed up to 189,000 infringement and counterfeiting cases.[10] Harmed by massive IP infringements, the

---

[6] G7 ICT and Industry Ministers' Declaration, Torino, Italy (September 25-26, 2017), at 14.
[7] The term "China" in this paper refers to the jurisdiction of mainland China ("People's Republic of China") only, and does not cover Hong Kong, Macau, or Taiwan.
[8] 2017 Situation Report on Counterfeiting and Piracy in the European Union, *supra* note 4, at 18.
[9] US Chamber of Commerce, Measuring the magnitude of global counterfeiting: creation of a contemporary global measure of physical counterfeiting, GIPC, Washington DC, 2016, p. 3. Available at: http://www.theglobalipcenter.com/wp-content/themes/gipc/map-index/assets/pdf/2016/GlobalCounterfeiting_Report.pdf.
[10] 2016 Intellectual Property Rights Protection in China, at 8. Available at: http://english.sipo.gov.cn/docs/2018-

development of IP industry in China is unhealthy. Without the support from its domestic IP enforcement and IP industry, the economy growth in China is decreasing in the recent years. For example, China paid up to USD 28.6 billion of royalties to foreign IPR owners in 2017.[11] As a result, China has the motivation to boost the competitiveness of its economy and to help the healthy development of its domestic IP industry. Nowadays, China is strengthening its IP protection by significant legal reforms.

After acceding to the World Trade Organization (WTO), China implemented its IP legal system by complying with WTO rules and kept reviewing and revising relevant laws, regulations and departmental rules in regards to IP protection. According to the China and World Trade Organization (June 2018)[12] published by the State Council Information Office of the PRC, China is improving its laws and regulations by setting up IP working mechanisms with many countries, drawing upon advanced intentional legislative practices, and building an IP system that suits national conditions of China.[13] Therefore, although IP infringement is a serious issue, China is improving its IP protection system and looking for international collaboration.

Although the economic motivation for China and other countries to build up IP working mechanisms is strong, network technology brings new challenges to IP protection in the digital world. With the development and popularization of network technology, an Internet user can easily access any digital online materials containing IP rights. Moreover, any Internet users can make the digital IP materials available through online intermediaries, usually Internet Service

---

01/20180131135159213892.pdf (last visited Aug. 28, 2018).

[11] CNNIC, 41st Statistical Report on Internet Development in China. http://cnnic.cn/hlwfzyj/hlwxzbg/hlwtjbg/201803/P020180305409870339136.pdf (last visited Sep 8th, 2018). English version is available at http://cnnic.com.cn/IDR/ReportDownloads/201807/P020180711391069195909.pdf.

[12] The State Council Information Office of the People's Republic of China (中华人民共和国国务院新闻办公室), *China and World Trade Organization* (《中国与世界贸易组织》白皮书). Available at http://www.scio.gov.cn/zfbps/32832/Document/1632334/1632334.htm (last visited Aug. 9th, 2018). English version is available at http://www.scio.gov.cn/zfbps/32832/Document/1632345/1632345.htm.

[13] China and World Trade Organization, Chapter I section 4, *supra* note 12, at 5.

Providers (ISPs), to the public without the authorization of the IP owners. As a result, counterfeit goods are increasingly distributed via online marketplaces and the online dissemination of protected content has been identified as a serious issue.[14]

B. IP Infringement issues of ISPs

1. IP liability of ISPs

Although ISPs may directly engage in IP infringement activities against IP owners, such as publishing copyright materials without copyright owners' authorizations, it is not difficult to locate ISPs according to the geographic locations of their server or the network locations of their domain names. However, for Internet users, it is easy for individual infringers to commit infringing activities through ISPs services or equipment. Due to the anonymity and non-geographic-boundary features of the Internet world, it could be extremely costly for the IP owners to trace and pursue legal actions against individual infringers over different corners of the world. As a result, since any Internet user can make copies of the original digital works and distribute them through the network, ISPs can easily be involved in IP infringements for making the unauthorized infringing materials available on their network. Therefore, it is likely that ISPs may commit secondary IP liability because of their users or subscribers, and this is a more controversial issue in the Internet and IP laws.[15]

Even though the ISPs are not directly responsible for any wrongdoing, IP owners usually take legal actions against ISPs rather than the end users. As the EU Copyright Directive concluded, "in many cases in the digital environment where, the services of intermediaries may increasingly be used by third parties for infringing activities, such intermediaries are best

[14] 2017 Situation Report on Counterfeiting and Piracy in the European Union, *supra* note 4, at 7.
[15] Although IP liabilities of ISPs include copyright, trademark, patent and trade secret, this dissertation only discusses copyright and trademark liabilities of ISPs due to the length of this dissertation.

placed to bring such infringing activities to an end."[16] Today, ISPs may be in the best position to stop IP infringements not only in the copyright regime, but also in other IP regimes such as trademark. Therefore, how to establish a unified IP liability system of ISPs is a key to IPR protection in digital economy.

IP owners usually demand strong protection over their IP rights, however, the Internet users and ISPs may accidentally access the infringing materials due to the availability of massive data on the network. In these circumstances, the ISPs are usually targeted as secondary infringers by the IP owners. However, IP enforcement against ISPs is difficult because the secondary liability system does not encourage ISPs to actively protect IPRs. As such, whether ISPs should actively prevent IP infringement for the IP owners is a controversial problem. Also, how to determine the liability of ISPs among different jurisdictions has become one of many global issues.

2. The Digital Millennium Copyright Act (DMCA) and the safe harbor doctrine

Although different countries have different approaches to solve IP liability issues of ISPs, in the copyright regime, many jurisdictions adopted the safe harbor doctrine that originated from the DMCA for many years.[17] The DMCA was enacted in 1988 when Internet was undeveloped. It was "designed to facilitate the robust development and world-wide expansion of electronic commerce, communications, research, development, and education in the digital age."[18] To promote the development of the Internet, the DMCA provides the safe harbor provision to shield ISPs from the secondary copyright infringement liability.[19] The safe harbor provisions of the DMCA requires IP owners to notify the ISPs by a specific form of

[16] Directive 2001/29/EC of the European Parliament and of the Council of May 22, 2001 on the Harmonisation of Certain Aspects of Copyright and Related Rights in the Information Society, Recital (59), 2001 O.J. (L 167) 10 (May 22, 2001).
[17] 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).
[18] S. REP. No. 105-190 at 1-2 (1998).
[19] 17 U.S.C. § 512(a)-(d).

notification in order to compel ISPs to remove the unauthorized infringing materials from their platforms in an expeditious and cost-effective way. After receiving notifications from the IP owners, the ISPs must remove the relevant materials from their platforms within expeditious period to be exempt from secondary liability. Following the DMCA, most ISPs establish Notice and Takedown (N&T) process for different IP regimes in order to obtain safe harbor protection. However, because nobody expected an extraordinary development of the Internet, the safe harbor doctrine has been criticized for lacking a balance among IP owners, ISPs and users.

For the IP owners, it is impossible for them to supervise all the ISPs in the world. Thus, the IP owners tend to send notifications without any considerations. To maximize the protection of their IP rights, it is likely that an IP owner would send notification that is beyond its actual IP rights, causing the abuse of the N&T mechanism. For the ISPs that lack incentive and ability to verify whether the notice is beyond the IP owner's actual right, they tend to execute the notification to avoid liability. For the Internet users, especially the subscribers of the ISPs, the abuse of N&T is likely to harm their lawful rights. To clarify this issue, two hypothetical cases will be discussed below.

For example, a copyright owner sent a notification to an ISP because the copyright owner finds unauthorized infringing materials on its website. Complying with the N&T provision, the ISP removed the material immediately and blocked the uploader's account. However, the unauthorized infringing materials may appear again on the website ISP because the infringer can create multiple user accounts to upload the infringing materials. The copyright owner has to find out the infringing materials and send the notification to the ISP again. A similar situation may happen again and again, and the ISP can always take advantage of the safe harbor doctrine to gain exemption from copyright liability. As a result, the copyright owner may very likely complain that the ISP "abused" the safe harbor doctrine in order to avoid secondary liability. Moreover, the same situation may also happen in the trademark regime,

and even worse, the N&T could be abused by sellers of the ISP.

Hypothetically, an ISP receives a trademark notification from one of its seller, A, claiming that another seller, B, is selling products that infringed A's trademark. Following the N&T provision, the ISP has to temporarily remove B's listings of the infringing products in order to verify whether (1) A owns or is authorized to use the trademark, and (2) B infringes A's trademark. However, A is a business competitor of B and abuses N&T for damaging B's online business. Even though B does not infringe A's trademark and its listings of products are recovered, B's online business is damaged during the period when the ISP is verifying the notification from A.

As a result, although the original purpose of the safe harbor doctrine is to "preserve [] strong incentives for service providers and copyright owners to cooperate to detect and deal with copyright infringements that take place in the digital networked environment,"[20] ISPs have less incentive to cooperate with IP owners and invest money and effort to actively protect IP now. To solve this dilemma, some jurisdictions are shifting from a passive-reactive approach to an active-preventive approach.[21]

3. Passive-reactive approach v. active-preventive approach

In a traditional passive-reactive model of ISPs, as long as the ISPs comply with the N&T policy and respond to the notification of infringement, they stay in safe harbor and are immune from IP liability from their subscribers. On the contrary, an active-preventive model requires ISPs to take active steps to prevent IP infringement on their platforms, which means more cooperation with IP owner. Although it is the IP owner's duty and right to protect its own IP rights, the ISPs bear more burden under an active-preventive model. For example, some jurisdictions adopted the Graduated Response procedure, also known as "three strikes and you are out" policy, which allows ISPs to terminate the repeated infringers' Internet connection of

[20] S. REP. No. 105-190 at 20 (1998); H.R. REP. 105-551(II), at 49 (1998).
[21] JEREMY DE BEER & CHRISTOPHER D. CLEMMER, *supra* note 17, at 377-378.

relevant ISPs.[22] Furthermore, in the EU, and lately Singapore and Australia, the IP owners can seek a Website Blocking Injunction from a court that compel ISPs to block access to infringing websites. Therefore, the trend of an active-preventive approach to ISPs is developing in many jurisdictions and how to rebalance the interests among Internet users, ISPs and IP owners is one of the subjects of this dissertation.

One of the other subjects is that whether establishing a unified IP protection system for ISPs is effective and appropriate in a digital age. Although both IP owners and ISPs desire an effective and harmonized legal framework to prevent IP infringements, a well-established ISP system in one IP regime may not work in another. For example, the DMCA stipulates safe harbor provisions for ISPs in the copyright regime,[23] however, whether the legislation should also provide a DMCA-like safe harbor rule in trademark regime is controversial. In *Tiffany (NJ) Inc. v. eBay Inc.*,[24] although eBay set up a N&T system where IP rights owner could notify eBay of potential infringing listings by filing a form, which is similar to the N&T system in the DMCA, the court struggled on whether it should apply a safe harbor rule for eBay in the trademark regime. Moreover, since the ISPs would respond to the trademark claims by removing the notified listing within twelve to twenty-four hours, business users of the ISPs could intentionally send trademark infringing claims for unfair competition purposes. The ISPs, however, do not have enough resources to verify each claim. Therefore, whether legally transplanting a DMCA-like safe harbor rule to the trademark regime in order to establish a unified IP protection system of ISPs is controversial.

---

[22] See, e.g., 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. 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.

[23] 17 U.S.C. § 512(a)-(d).

[24] *Tiffany (NJ) Inc. v. eBay Inc.*, 600 F.3d 93 (2d Cir. 2010).

C. The Electronic Commerce Law of the PRC

In China, the Electronic Commerce Law of the PRC (E-commerce Law)[25] set up a comprehensive mechanism of ISPs, including a unified IP protection system for ISPs. This new law was promulgated in 2018 and constituted a blueprint for the mechanism of ISPs. In the area of IP, first, the E-commerce Law adopts an active-preventive approach and requires ISPs to actively protect IPRs.[26] According to Article 41 to 45 of the E-commerce Law, ISPs have to establish a unified N&T policy in all IP regimes to actively prevent infringements.[27] Second, Article 5 of the E-commerce Law innovatively established the construction for a unified IP protection system of ISPs, which includes the E-commerce Law, IP laws, IP-related laws and administrative enforcements.[28] In other words, not only does the E-commerce Law require ISPs to comply with the active-preventive model that set up from Article 41 to 45, but also require ISPs to comply with other doctrines in according to other laws or administrative enforcements. For example, Article 5 of the E-commerce Law requires ISPs to abide by IP laws and IP-related laws, such as the doctrine of anti-unfair competition law. As a result, the E-commerce Law provides legal certainty for IP infringement issues of ISPs, and sets up a blueprint for Chinese legislation to improves IP protection system of ISPs by amending other relevant laws or administrative enforcements.

Although the new E-commerce Law innovatively establishes the construction of a

---

[25] Zhong hua ren min gong he guo dian zi shang wu fa (中华人民共和国电子商务法) [Electronic Commerce Law of the People's Republic of China] (promulgated by the Standing Comm. Nat'l People's Cong., Aug. 31, 2018, effective in Jan. 1, 2019) [hereinafter E-commerce Law].

[26] E-commerce Law, *supra* note 25, art. 41: "E-commerce platform operators shall establish rules for protecting intellectual property rights, strengthening cooperation with intellectual property rights holders to lawfully protecting intellectual property rights."

[27] E-commerce Law, art. 41-45.

[28] E-commerce Law, art. 5: "E-commerce operators shall carry out business activities according to the principles of voluntariness, equality, fairness and integrity, abide by laws and business ethics, participate in market competition fairly, fulfill their obligations in terms of consumer rights protection, environmental protection, intellectual property right protection, as well as network security and personal information protection, undertake responsibilities related to the quality of products and services, and accept the supervision of the government and society."

unified IP protection system for ISPs, this new unified system is incomplete and demands further improvement. For example, Internet Content Providers are not included in the E-commerce Law,[29] and the Chinese legislation plans to enact relevant provisions in the Third Amendment of the Copyright Law in the future.[30] This dissertation analyzes the impact of this new E-commerce Law to ISPs, and proposes suggestions to Chinese legislation on how to improve the unified IP protection system of ISPs in China.

D. Overview

This dissertation engages in a critical review of the secondary liability of ISPs as a hub for the protection and enforcement of IP rights, with a specific focus on developments that recently take place in China within the larger legal framework of the countries that have adopted an active-preventive model.

In terms of structure, this dissertation consists five chapters. Chapter II introduces how different jurisdictions define ISPs in different approaches. Then demonstrates the development on how Chine defines ISP in different laws and regulations. Chapter III presents the development of secondary liability of ISPs in the copyright regime. Chapter IV analyzes the legal theory of ISPs' secondary liability in the trademark regime and the anti-unfair competition approach of ISPs in China. With a focus on major cases about giant ISPs in China and the U.S., such as BAT (Baidu, Alibaba, Tencent), Google and eBay, this Chapter illustrates the shortcomings of the N&T system in the trademark realm and provides a proposal of legal reforms in China. Chapter V examines several active-preventive approaches of ISPs, with a

[29] E-commerce Law, art. 2 para. 3.

[30] See e.g. Zhong hua ren min gong he guo zhu zuo quan fa (xiu ding fa an song sheng gao) [中华人民共和国著作权法(修订草案送审稿)] [Draft of the Copyright Law of the PRC (2014)] (published by the Legislative Affairs Office of the State Council of the PRC) [hereinafter 2014 Copyright Draft]. Available at https://npcobserver.files.wordpress.com/2017/08/copyright-law-2014-draft-revision.pdf.

special focus of the Website Blocking Injunction. By exploring whether a blocking injunction system could prevent online IP infringement more effectively, this chapter provides a proposal of legal reforms the improve the unified IP protection system of ISPs in China. Chapter VI generates a conclusion for the legal reform of ISPs in China.

Chapter II: Defining ISPs

Because there is no universal definition of ISPs in the world, this chapter presents how International treaties and different jurisdictions defining ISPs, with a specific focus on the new definition of ISPs in the E-commerce Law. Before discussing the definition of ISPs in the E-commerce Law, this chapter introduces how different jurisdictions define ISPs with different approaches. Then a comparative research methodology will be used when analyzing the benefits and drawbacks of the definition in the E-commerce Law.

Part A of this chapter introduces different approaches on defining ISPs in various jurisdictions, especially the definition of ISPs in the DMCA. Part B presents how China follows the DMCA approach by defining ISPs in different laws and regulations, then compare the approach of ISPs in China with the approaches of ISPs in other jurisdictions. Part C presents how China defines ISPs in two new Internet laws, with a special focus on the new E-commerce Law. Part C also discusses the potential legal contradiction of the definition of ISPs in the E-commerce Law, then analyzes the impact of the new definitions of ISPs in China by examining legislature history of the E-commerce law.

A. The Definitions of ISPs

1. International treaties

The World Intellectual Property Organization (WIPO) administered two treaties in 1996: WIPO Copyright Treaty (WCT) and WIPO Performance and Phonogram Treaty (WPPT). Known together as the "Internet Treaties," they are considered the first international agreements to deal with Internet intermediary issues within the copyright regime. Although there is no specific definition for ISPs, Article 2 of WPPT[31] and Article 8 of WCT indicate that

[31] WIPO Performance and Phonogram Treaty, art. 2 section (f): "'broadcasting' means the transmission by wireless means for public …"

ISPs could be any intermediaries that provide online services to the public through wire or wireless means.[32] These provisions also grant copyright owners some exclusive rights to prevent online infringements. Any activity that makes copyright work available to the public, without authorization by the copyright owner, is considered copyright infringement. However, ISPs are likely engaged in infringing activities because their subscribers use their services and equipment. Therefore, these exclusive rights could be too harsh to ISPs. To restrict these exclusive rights of copyright owners 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 . . . ," which provides a safe harbor for network intermediaries such as ISPs.

2. Definitions of ISPs in different jurisdictions

Most of the jurisdictions define ISPs in their Copyright Acts. For example, in the U.S., the Digital Millennium Copyright Act (DMCA) was enacted on Oct. 28, 1998. Section 512 of the DMCA illustrates four categories of "service providers": (1) transitory digital network communication; (2) system caching; (3) information residing on system or network at direction of users; and (4) information location tools.[33] Section 512(k)(1) of the DMCA stipulates two definitions of ISPs, one narrow and one broad. Section 512(k)(1)(A)[34], which is narrowly defined, only applies to ISPs that falls under this section. 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)."[35] The main drawback of defining ISPs in copyright law is that the definition cannot cover other IP regimes,

[32] WIPO Copyright Treaty, art. 8: "… the exclusive right of authorizing any communication to the public of their work, by wire or wireless means."
[33] 17 U.S.C. § 512(a)-(d).
[34] 17 U.S.C. § 512(k)(1)(A): "As used in subsection (a), the term "service provider" means 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."
[35] 17 U.S.C. § 512(k)(1)(B).

such as trademark. Therefore, some jurisdictions define ISPs outside IP laws.

Some jurisdictions define their ISPs in Telecommunication Acts in a broad way. For example, in Japan, 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]."[36] This is a broad definition compared to that defined by the U.S. law.

Some jurisdictions also define their ISPs in Telecommunication Act and distinguish ISPs into different categories. For example, in Australia, Article 86 of Telecommunications Act stipulates that "a service provider is: (a) a carriage service provider; or (b) a content service provider."[37] Article 87 of Telecommunications Act define a carriage service provider[38] as an Internet apparatus provider that provide essential apparatuses or fundamental communication services for network operation. Article 97 of Telecommunications Act defines a content service provider[39] as an Internet content provider that facilitate the transmission of information between end users. Some jurisdictions, however, do not have a clear definition of ISPs.

---

[36] 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 is available at http://www.japaneselawtranslation.go.jp/law/detail/?id=2088&vm=04&re=01&new=1.

[37] Article 86 of *Telecommunications Act 1997* (Cth) pt 4 div 3 (Austl.).

[38] Article 87 of *Telecommunications Act 1997* (Cth) pt 4 div 3 (Austl.): "(1) For the purposes of this Act, if a person supplies, or proposes to supply, a listed carriage service to the public using: (a) a network unit owned by one or more carriers; or (b) a network unit in relation to which a nominated carrier declaration is in force; the person is a carriage service provider."

[39] Article 97 of *Telecommunications Act 1997* (Cth) pt 4 div 4 (Austl.): "(1) For the purposes of this Act, if a person uses, or proposes to use, a listed carriage service to supply a content service to the public, the person is a content service provider."

B. Defining ISPs in China before new promulgated Internet Laws

This section introduces how China follows the DMCA and defines ISPs in different laws and regulations, and then demonstrates why there are no clear definitions of ISPs before two new promulgated Internet Laws.

1. Copyright Law

From a historical perspective, Chinese legislature has followed the DMCA and stipulated ISPs-related provisions in the different Chinese laws and regulations. The Copyright Law of the RPC (hereinafter "2010 Copyright Law")[40] was revised twice. The first revision in 2001, the Copyright Law was revised to qualify the minimum protection standard of the TRIPS Agreement.[41] The second revision in 2010, it was revised to fulfill the ruling of WTO about IP issue between China and the U.S.[42] One of the most important rights for copyright owners is "the right to communicate works to the public over information networks" (right of dissemination via information network).[43] According to Article 59 of the 2010 Copyright Law, "right of dissemination via information network shall separately formulated by the State Council."[44] Therefore, there is no further interpretation about the right of dissemination via information network in the amended 2010 Copyright Law. In 2013, the State Council enacted ISPs-related provisions in the Regulations on the Protection of Right of Dissemination via

---

[40] 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) [hereinafter 2010 Copyright Law]. The English translation is available at http://www.cpahkltd.com/EN/info.aspx?n=20100429164418197504.

[41] Agreement on Trade-Related Aspects of Intellectual Property.

[42] Wu Handong (吴汉东*), The Background, Layout and emphasis on the Third Amendment of the Copyright Law*, (《著作权法》第三次修改的背景、体例和重点), Law and Business Research (法商研究), issue 4, 2012 at 4.

[43] 2010 Copyright Law, art. 10: "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."

[44] 2010 Copyright Law, art. 59.

Information Network (RPRD).[45]

2. RPRD

The RPRD is a regulation about the right of dissemination via information network under the 2010 Copyright Law. Similar to Section 512(a) to (d) of the DMCA, the RPRD illustrates four categories of "network service providers" (i.e. ISPs): (1) network automatic access service or automatic transmission service;[46] (2) automatic caching;[47] (3) information storage space;[48] and (4) search or link service.[49] However, unlike the DMCA that provides two definitions in section 512(k)(1), there is no clear definition of ISPs in the RPRD. Article 14 of the RPRD stipulates that "a network service provider that provides information storage space or provides searching and linking services . . ."[50] is only an illustration of ISPs rather than a definition. The scope of the concept remains uncertain. Likewise, the Tort Liability Law of the PRC[51] has the same definition issue of the "network service provider." Article 36 of the Tort Law stipulates the tort liability of "network service provider," but there is no definition about "network service provider" in the Tort Law.[52]

Moreover, the lack of clear definition for ISPs may cause huge uncertainties for legal practice, especially when mere illustration of ISPs in the RPRD cannot apply to later-developed technology. For example, the question of whether P2P technology should be applied to the four categories of ISPs in Section 512 has been raised in the U.S. courts.[53] Likewise, the People's

---

[45] Xin xi wang luo chuan bo quan bao hu tiao li (信息网络传播权保护条例) [Regulations on the Protection of the Right of Dissemination via Information Network] (promulgated by the St. Council, May 18, 2006, amended by the St. Council in Jan 30, 2013) [hereinafter RPRD]. The English translation is available at http://www.cpahkltd.com/UploadFiles/20100315165559735.pdf.
[46] RPRD, *supra* note 45, art. 20.
[47] RPRD, art. 21.
[48] RPRD, art. 22.
[49] RPRD, art. 23.
[50] RPRD, art. 14.
[51] 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 Liability Law of the PRC] (promulgated by the Standing Comm. Nat'l People's Cong., Dec. 26, 2009, effective in Jul. 1, 2010) (China). Translated by Westlawchina (www.westlawchina.cn) [hereinafter Tort Liability Law].
[52] Tort Liability 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."
[53] Metro-Goldwyn-Mayer Studios Inc. v. Grokster Ltd., 125 S. Ct. 2764 (2005). See also A&M Records v. Napster, 239 F.3d 1004 (9th Cir. 2001).

Courts in China also struggled by whether P2P technology should be applied to the four categories of ISPs in the RPRD.[54] As a result, the People's Court in China tried to solve this problem through case law.

3. Case law

In Chinese case law, Judge Zhou Xiaobin of the Beijing Second Intermediate People's Court drew a conclusion from a copyright case.[55] He concluded that the Internet infrastructure service providers could be divided into three major categories: Internet content provider, online service provider, and Internet apparatus provider. Internet content providers select, edit, and upload information content; online service providers facilitate the transmission of information without selecting or editing the contents; Internet apparatus providers provide essential apparatuses for network operations. However, since case law is not binding in China, the definition of ISPs within the case law is merely a reference for the Chinese legislature. Moreover, technology usually develops beyond the law. Mere three categories of ISPs may not be enough to cover new ISPs created by future technologies or businesses. Therefore, it is foreseeable that the law should define ISPs in a broad way to cover not only the current three major categories of ISPs, but also potential categories in the future. Furthermore, because ISPs may engage in different IP regimes, only defining ISPs in copyright law can be problematic.

Mere definition of ISPs in copyright law can be insufficient because an ISP is likely to engage in different IP regimes, such as trademark. Today, a single application of a smart phone can provide multiple services, and therefore, engage in infringements in different IP regimes. For example, WeChat (i.e. WeiXin) is considered a popular Chinese mobile messaging-social, network-payments, and network-services application that is provided by Chinese technology giant Tencent Holdings, Ltd. (hereinafter "Tencent"), with more than 1 billion users. One of

---

[54] *See Guangdong Zhongkai Culture Development Ltd. v. Guangzhou Shulian Software Technology Ltd.*, Shanghai High Court (2008) Hu gao min san zhi Zhong zi di No. 7.

[55] *See 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.

the significant features of WeChat is its "Mini Programs" function that allows other ISPs to provide their services to WeChat users. Not only can WeChat users share or post copyright contents online like a traditional social-network (such as Facebook), but it can also provide services from other ISPs through Mini Programs (such as eBay & Amazon). As a result, WeChat could be involved in both copyright and trademark infringements.

Accordingly, trademark infringement has been an issue for Tencent. For example, founded by Tencent in 2015, Pinduoduo Inc. is a third-party e-commerce platform with over 300 million active users. It sells discounted products by incorporating social networking (i.e. WeChat) with online shopping. Many consumers and trademark holders have complained that Pinduoduo is selling counterfeits and replicas of branded products.[56] In this case, mere definitions of ISPs in copyright regime are insufficient to solve the ISPs issues. Consequently, enlarging the scope of ISPs and defining ISPs in a broad way to cover all IP regimes has been raised by Chinese legal scholars.[57]

4. Proposal from Chinese legal scholars

Since the lack of a clear definition may cause huge uncertainties for legal liability, many Chinese scholars try to define ISPs from an academic perspective.[58] For example, 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.[59] Since Japan is also a civil law country like China and the ISP definition from Japan is broad, the Chinese legislature could consider legally transplanting the Japanese ISP definition. However, Chinese legislature did not adopt the Japanese approach but followed the U.S. approach and stipulated two definitions of ISPs in two new promulgated Internet laws,

---

[56] Liang Jun & Bianji, *China probes online group discounter Pinduoduo over counterfeit allegation*, Xinhua (新华网) (Aug. 2, 2018, 08:29), http://en.people.cn/n3/2018/0802/c90000-9486961.html.
[57] 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 100.
[58] Luo, *supra* note 57, at 96.
[59] Luo, *supra* note 57, at 99.

which will be discussed below.

C. Definitions of ISPs in two new promulgated Internet Laws

This section demonstrates how China defines ISPs in two Internet laws: a broad definition in the Network Security Law of the PRC (Network Security Law)[60] and a narrow definition in the E-commerce Law. Article 2 of the E-commerce Law provides several exceptions for ISPs, which narrows the scope of ISPs in E-commerce Law. However, these exceptions in Article 2 is controversial to the purpose of the E-commerce Law and may contradict with Article 41 of the E-commerce Law. Therefore, Section 2 analyzes the legislature history of the E-commerce law and indicates that the purpose of the Chinese legislation is to define ISPs in a broad way while avoiding legal conflicts with the existing and future laws and regulations. Section 3 further discusses the impact of the E-commerce Law for ISPs in China.

1. Network Security Law

Because of the lack of a clear definition of ISPs in China before 2017, the Network Security Law defined ISPs in a broad way. With the development of network technology and the wave of Web 2.0, the Chinese legislature noticed that it is necessary to stipulate Internet laws for the new legal environment in the information age. The Network Security Law was promulgated in 2016 and made effective in 2017. Instead of using the "network service providers" in the Tort Law and the RPRD, Article 76 section 3 defines ISPs as "network operators," and includes the "network service providers" by providing that: "network operators shall refer to the owners and managers of networks and the network service providers."[61] Thus,

[60] Zhong hua ren min gong he guo wang luo an quan fa (中华人民共和国网络安全法) [Network Security Law of People's Republic of China] (promulgated by the Standing Comm. Nat'l People's Cong., Nov 7, 2016, effective Jun 1, 2017 [hereinafter the Network Security Law]. The English translation is available at http://app.westlawchina.com/maf/china/app/document?&docguid=i0000000000000158419794ee47c2ec4f&hitguid=i0000000000000158419794ee47c2ec4f&srguid=i0ad82a41000001654e10c1bcf705f670&spos=1&epos=1&td=122&crumb-action=append&context=21&lang=en).

[61] Network Security Law, art. 76 (3).

the "network operators" of the Network Security Law is a broader definition than the definitions of "network service providers" in Tort Law and the RPRD. Moreover, because "the owners and managers of networks" could refer to any online business entities that "apply to the construction, operation, maintenance and use of networks as well as the supervision and administration of network security within the territory of the PRC,"[62] which almost brings all the categories of ISPs into its scope.

Nonetheless, the Network Security Law still does not provide a clear definition for the "network service providers." Moreover, the Network Security Law does not stipulate specific IP liabilities for ISPs. Article 12 of the Network Security Law merely provides a legal foundation on ISPs' IP liabilities, which states that any individuals and organizations that use networks shall not endanger network security or make use of networks to engage in activities such as infringing Intellectual Property rights.[63] As a result, although the Network Security Law defines ISPs in a broad way, it does not provide any specific IP-related provisions.

2. E-commerce Law

E-commerce maintained a rapid growth in China from 2013. According to the 41st Statistical Report on Internet Development in China (Jan 2018)[64] from China Internet Network Information Center (CNNIC), online retails sales in China reached a record high of RMB 7.18 trillion (approximately USD 1.05 trillion) in 2017,[65] which is the biggest e-commerce trade

---

[62] Network Security Law, art. 2.

[63] Network Security Law, art. 12. "The State shall protect the rights of citizens, legal persons and other organizations to use networks in accordance with the law, promote the popularity of network access, improve network service level, provide the public with safe and convenient network services, and guarantee the legal, orderly and free flow of network information.
Any individuals and organizations that use networks shall comply with the Constitution and laws, abide by public order and respect social morality and shall not endanger network security or make use of networks to engage in the activities such as endangering national security, honor and interests, inciting the subversion of the State political power and the overthrow of the socialist system, inciting plit of the state, undermining national unity, propagating terrorism, extremists, racial hatred or ethnic discrimination, spreading violent and pornographic information, fabricating and spreading false information to disrupt economic order and social order, and infringing the reputation, privacy, intellectual property rights and other lawful rights and interests of other people."

[64] CNNIC, 41st Statistical Report on Internet Development in China, *supra* note 11.

[65] CNNIC, 41st Statistical Report on Internet Development in China, *supra* note 11, at 67.

volume in the world. In particular, online retail sales of physical goods reached RMB 5.4806 trillion (approximately USD 0.8 trillion). However, popular e-commerce platforms such as Alibaba's Taobao has long been criticized for providing a platform for counterfeits and scams. Moreover, online services are also part of the e-commerce in China. ISPs that provide online services such as online content providers were also reported infringing copyright, including "the publishing and selling of pirated books, and unlicensed distribution of literature, music, games and audiovisual products on the Internet."[66] Nonetheless, relevant laws concerning e-commerce were nonexistent before 2018. To regulate the online market and protect legal rights and interests of all parties, the E-commerce Law of PRC was promulgated in August 31, 2018 and made effective January 1, 2019. It defines ISPs in a broad way to cover online businesses in e-commerce.

Similar to the Network Security Law, the E-commerce Law also defines ISPs by a new term "e-commerce operators" instead of the "network service providers." Article 9 of E-commerce Law defines e-commerce operators as "…any natural persons, legal persons or other organizations that sell goods or provide services through the Internet or other information networks.[67] E-commerce operators include e-commerce platform operators[68], intra-platform operators[69] and other e-commerce operators who sell merchandise or provide services through self-built websites or other web services.[70] Thus, Article 9 of the E-commerce Law defines ISPs in a broad way, which covers almost all the online businesses that is related to e-commerce. Moreover, as mentioned in Chapter I, Article 41 of the E-commerce Law requires e-commerce

[66] Du Mingming, Bianji, Chinese copyright regulator publicizes piracy cases, Xinhua (新华网), (April 27, 2017 09:07), http://en.people.cn/n3/2017/0427/c90000-9208308.html
[67] E-commerce Law, art. 9.
[68] E-commerce Law, art. 9, para. 2: "As used in this law, e-commerce platform operators mean any legal persons or unincorporated organizations that provide two or more parties to a transaction in e-commerce with services such as network business venues, deal makings, and information distribution for the two or more parties to the transaction to independently carry out business activities."
[69] E-commerce Law, art. 9, para. 3: "As used in this law, infra-platform operators mean e-commerce operators who sell merchandise or provide services on e-commerce platforms."
[70] E-commerce Law, art. 9.

platform operators to cooperate with right holders and establish rules for IPR protection,[71] which sets up legal obligations for ISPs to actively protect IP. As a result, not only does the E-commerce Law clearly stipulate the definition of ISPs, but it also stipulates the IP liabilities of ISPs.

However, the definition of ISPs in the E-commerce Law is narrower than the definition of ISPs in Network Security Law because Article 2 of the E-commerce Law provides the scope of the "e-commerce" by listing serval exceptions. These exceptions are arguable because not only do they narrow the scope of e-commerce operators under the E-commerce law, but also seems to contradict the purposes of Article 5 and 41 of the E-commerce Law requiring ISPs to protect IPRs. These exceptions and the legislature purpose of Article 2 will be analyzed below.

a. Definitional exceptions of "e-commerce"

According to the CNNIC reports, the online retail sales of physical goods is only part of the e-commerce in China. Most of the giant ISPs such as Amazon also provides content services such as Amazon Music, Amazon Video, Kindle E-books, etc. Therefore, the scope of "e-commerce" in the E-commerce Law should be broad to cover all online businesses, otherwise the scope of "e-commerce operators" in Article 9 would be too narrow to cover different ISPs in e-commerce. Notwithstanding, although the second paragraph of Article 2 stipulates that "e-commerce means doing business over information networks such as the Internet, including activities of selling products or providing services," the third paragraph stipulates that "this law is not applicable to financial products and services;[72] the use of information networks to provide content services such as news information, audio-visual programs, publications and cultural products."[73] In other words, the second paragraph of

[71] E-commerce Law, art 41.
[72] The "financial products and services" will not be discussed because they are less relevant to IP.
[73] E-commerce Law, art. 2.

Article 2 defines e-commerce to cover all online business involving e-commerce, but the third paragraph excludes some online content services, which are part of business in e-commerce, from the definition. Therefore, it is debatable to exclude the online content services from the scope of e-commerce. The reasons why online content services should not be excluded from the E-commerce Law will be discussed below.

First, excluding some online content services from the E-commerce Law does not correspond to the huge online content market in China. Internet content services such as online news, music, literature and video, have been a growing business of Chinese e-commerce. According to the 41st Statistical Report on Internet Development in China, as of December 2017, China has 647 million of online readers,[74] 548 million of online music users,[75] 378 million of online literature users,[76] and 579 million of online video users.[77] For such a big online market, laws that regulate online content services is necessary for the Chinese online market. Therefore, excluding Internet content services from E-commerce law may cause uncertainties for ISPs' legal liabilities.

Second, online piracy is a huge problem in China. As mentioned in the last Chapter, online environment for the content services in China is horrible. Since 2010, China has launched a month-long anti-piracy campaign every year.[78] For example, in 2017, Chinese administrative launched the "Sword Net Campaign"[79] for combating online infringement and piracy. According to the report of "Sword Net Campaign 2017"[80] from the National Copyright Administration of the PRC (NCAC), the law enforcement departments shut down 2554

[74] CNNIC, 41st Statistical Report on Internet Development in China, *supra* note 11, at 35.
[75] CNNIC, 41st Statistical Report on Internet Development in China, *supra* note 11, at 43.
[76] CNNIC, 41st Statistical Report on Internet Development in China, *supra* note 11, at 44.
[77] CNNIC, 41st Statistical Report on Internet Development in China, *supra* note 11, at 46.
[78] Jiang Jie, China highlights IPR protection to encourage creativity, People's Daily Online, (12:03, Aug. 23, 2018) available at http://en.people.cn/n3/2018/0823/c90000-9493519.html (last visited Oct. 23, 2018).
[79] China and World Trade Organization, Chapter I section 4, *supra* note 12, at 6.
[80] National Copyright Administration of the PRC (中华人民共和国国家版权局), *Report of the "Sword Net Campaign 2017,"* ("剑网 2017"专项行动的有关通报) Jan 16, 2018. Available at http://www.ncac.gov.cn/chinacopyright/contents/10873/357502.html.

infringing piracy websites, blocked 0.710 million infringing piracy links, captured 2.76 million infringing piracy products, amounting to RMB 107 million (approximately USD 15.6 million). The report specifically pointed out that the law enforcement departments shall focus on e-commerce platforms to shut down the online sales channels of infringing piracy duplicate.[81] Therefore, it is essential that the E-commerce law should pinpoint the online piracy issues on the e-commerce platforms.

Third, excluding the online content services in Article 2 of the E-commerce Law contradicts the purpose of Article 41 that requires e-commerce platform operators to cooperate with right holders and to establish rules for IPRs protection.[82] Because the online content services require copyright protection and Article 41 intends to strengthen IPRs protection, ISPs that provide content services perfectly fulfill the purpose of Article 41. Therefore, it seems unreasonable to exclude online content services from E-commerce Law.

As a result, excluding Internet content services from E-commerce law may cause huge uncertainties for legal liabilities, especially in the online copyright regime. To resolve why Chinese legislature excludes Internet content services from the E-commerce law, next section will analyze the legislature history of the E-commerce law.

b. Legislature history of the E-commerce law

From December 2013, the Financial Affairs Committee of the National People's Congress (NPC) started the legislation draft of the E-commerce law to regulate the burgeoning e-commerce in China and thereby facilitating growth, maintaining "market order", and eradicating scams and counterfeits. After a three-year investigation, the first draft of the E-commerce Law was submitted to the Standing Committee of the NPC for deliberation on December 27, 2016. According to the "Explanation on the Draft of E-commerce Law of the

[81] NCAC (国家版权局), *Report of the "Sword Net Campaign 2017,"* ("剑网 2017"专项行动的有关通报), *supra* note 80.
[82] E-commerce Law, art. 41.

PRC,"[83] the vice chairman of the Financial Affairs Committee of the NPC Lü Zushan explained that the legal entity of the E-commerce law should fully consider "covering the practical area of e-commerce and effectively connecting with other laws and regulations." Therefore, the first draft of the E-commerce law "does not apply to financial products or services, and the use of information networks to provide content services such as audio-visual programs and online publications etc."[84] According to the explanation of the first draft, the "other laws and regulations" may refer to the existing laws and regulations that provide online finance-related provisions and online copyright-related provisions. Therefore, the Chinese legislature may intend to limit the scope of the E-commerce law by excluding financial services and content services from the definition of e-commerce. Also, a narrow definition of e-commerce law can avoid legal conflicts with existing laws and regulations.

Moreover, the modification of the drafts of the E-commerce law of and their related legal materials are also critical to determine the purpose of the Chinese legislature on excluding financial services and content services from the E-commerce law. In October 2017, the Second Deliberation Draft of the E-commerce law[85] expands the exceptions of e-commerce by adding "Internet cultural products"[86] onto the content services list. Moreover, the Third Deliberation Draft of the E-commerce law[87] further expands the exceptions of e-commerce by adding

---

[83] Lü Zushan, *Explanation on the draft of E-commerce Law of PRC*, No. 12 Standing Comm. Nat'l People's Cong., Meeting No. 25, Nov 19, 2016. Available at http://www.npc.gov.cn/npc/xinwen/2018-08/31/content_2060159.htm.

[84] Zhong hua ren min gong he guo dian zi shang wu fa (cao an) [中华人民共和国电子商务法(草案)] [First Draft of the E-commerce Law (Dec 2016)] (published by the Standing Comm. Nat'l People's Cong. in Dec. 2016), available at https://npcobserver.files.wordpress.com/2016/12/e-commerce.pdf.

[85] Zhong hua ren min gong he guo dian zi shang wu fa (er ci sheng yi gao) [中华人民共和国电子商务法(二次审议稿)] [Second Deliberation Draft of the E-commerce Law (Oct 2017)] (published by the Standing Comm. Nat'l People's Cong. in Oct. 2017), available at https://npcobserver.files.wordpress.com/2017/11/e-commerce-law-2nd-draft.pdf.

[86] Second Deliberation Draft of E-commerce Law of PRC, art. 2: "… This law does not apply to financial products and services; the use of information networks to provide content services such as audio-visual programs and online publications, Internet cultural products, etc."

[87] Zhong hua ren min gong he guo dian zi shang wu fa (san ci sheng yi gao) [中华人民共和国电子商务法(三次审议稿)] [Third Deliberation Draft of the E-commerce Law (Jan 2018)] (published by the Standing Comm. Nat'l People's Cong. in Jan 2018), available at https://npcobserver.files.wordpress.com/2018/06/e-commerce-law-3rd-draft.pdf.

"news information"[88] onto the content services list. As a result, the Chinese legislature keeps narrowing the scope of the e-commerce by expanding the exception lists. The reports of the later drafts confirm the purpose of the Chinese legislature is to limit the scope of the E-commerce law.

First, according to the "Report of the NPC Law Committee to amend the Draft of the E-commerce law of PRC," in October 2017, the NPC Law Committee believes "for the provisions that have already stipulated in the existing related laws, this law shall not stipulate again, also shall reserve or add connecting provisions of the related laws."[89] This report indicates that the Copyright Law of PRC and related regulations have stipulated provisions for online content services, therefore, shall not be stipulated again in the E-commerce law.

Second, the "Report of the NPC Law and Constitution Committees to amend the Draft of the E-commerce law of PRC" confirms that "[this law] shall manage the relationship with related Civil Laws and administration regulations. For the provisions that have clearly stipulated in the existing laws, [this law] shall not stipulate again."[90] As mentioned in the previous section, the 2010 Copyright Law, the Tort Liability Law and the RPRD stipulates related provisions of content services via information networks. Therefore, it is possible that the Chinese legislature excludes some online content services form E-commerce law because the related provisions exist in current laws and regulations.

Third, the report also mentioned that the E-commerce law does not apply to content

---

[88] Third Deliberation Draft of E-commerce Law of PRC, art. 2: "… This law does not apply to financial products and services; the use of information networks to provide content services such as news information, audio-visual programs and online publications, Internet cultural products, etc."

[89] NPC Law Committee (全国人民代表大会法律委员会), *Report of the NPC Law Committee to amend the Draft of the E-commerce Law of the PRC* (全国人民代表大会法律委员会关于《中华人民共和国电子商务法(草案)》修改情况的汇告), Oct 31, 2017. Available at: http://www.npc.gov.cn/npc/xinwen/2018-08/31/content_2060144.htm.

[90] NPC Constitution and Law Committees (全国人民代表大会宪法和法律委员会), *Report of the NPC Constitution and Law Committees to amend the Draft of the E-commerce Law of the PRC* (全国人民代表大会宪法和法律委员会关于《中华人民共和国电子商务法(草案)》修改情况的汇告), Jun 19, 2018. Available at: http://www.npc.gov.cn/npc/xinwen/2018-08/31/content_2060320.htm.

services because of the "specialties of the industry and field."[91] It is possible that the Chinese legislature is concerned about the legal issues of copyright in the network environment. For example, Article 22 of the 2010 Copyright Law[92] provides serval fair use situations including "news reporting,"[93] "publication"[94] and "cultural products."[95] Whether the scope of fair use doctrine in the 2010 Copyright Law should cover online news, publication and cultural products is controversial. As a result, because the copyright issues of online content services remain unresolved, it is possible that the Chinese legislature excludes them from the E-commerce Law because of the Third Amendment of the Copyright Law. This hypothesis will be discussed below.

c. Third Amendment of the Copyright Law

As mentioned before, the existing provisions that related to the online content services in the 2010 Copyright Law and the RPRD might not effectively protect copyrights online. Currently China is working on amending its copyright law and trying to solve massive online copyright infringement issues.[96] According to the Draft of the Copyright Law of the PRC (hereinafter "2014 Copyright Draft"),[97] the Chinese legislature is trying to stipulate provisions that relate to online content services in the Third Amendment of the Copyright Law.

According to the Copyright Draft, Chinese legislature plans to narrow the scope of the

---

[91] NPC Constitution and Law Committees, *Report of the NPC Constitution and Law Committees to amend the Draft of the E-commerce Law of the PRC*, *supra* note 90.
[92] 2010 Copyright Law, art. 22: "Under the following circumstances, a work may be used without authorization from the copyright owner and without payment of remuneration thereto, provided that the author's name and the title of the work shall be indicated and other rights to which the copyright owner is entitled under this Law shall not be infringed:"
[93] 2010 Copyright Law, art. 22 Item (3): "An inevitable show or citation of a published work via a medium such as a newspaper, periodical, radio channel, or television channel, for reporting news on current events."
[94] 2010 Copyright Law, art. 22 Item (2): "A proper citation of others' published works in a work for introducing, or commenting on, a particular work or for elaborating on a particular question."
[95] 2010 Copyright Law, art. 22 Item (11): "Translating a published work created in the Chinese Han language by a Chinese citizen, legal person or other organization into a written work in a language used by a domestic minority nationality for publishing and distribution in China."
[96] China and World Trade Organization, Chapter I section 4, *supra* note 12, at 6.
[97] 2014 Copyright Draft, *supra* note 30.

safe harbor doctrine, therefore, strengthen the online copyright protection. First, Paragraph 1 Article 73 of the Copyright Draft adopts the ISPs related provisions in the RPRD.[98] It provides that "when network service providers merely provide network technical services, such as information storage space or provides searching and linking services to network users, they do not bear the duty of examining copyright and its related rights."[99] Because the RPRD is a regulation for trial implementation, the Chinese legislature plans to transplant the safe harbor doctrine from the RPRD to the Third Amendment of Copyright Law. Second, Paragraph 5 Article 73 of the Copyright Draft provides that "it is not applicable to Paragraph 1 of this article if network service providers provide to the public the works, performances, or audio-visual recordings of others through information networks."[100] This paragraph excludes the Internet content providers from the safe harbor doctrine. In other words, it narrows the scope of the safe harbor doctrine so that Internet content providers are no longer able to abuse the safe harbor doctrine in order to avoid copyright liability. Chapter III discusses this copyright liability issues of ISPs in detail. Now the Copyright Draft is under deliberation in the Standing Council of NPC.

3. The impact of the new definitions of ISPs in China

Although different Chinese laws and regulations define ISPs in various terms, the definitions of ISPs and the scope of IPR protection are distinct. The broadest definition of ISPs in Network Security Law defines network operators as the owners and managers of networks and the network service providers, with a full coverage of IPR protection. A narrower definition of ISPs in E-commerce Law defines e-commerce operators as any entity that sells goods or provides services through the Internet or other information networks, with exceptions on Internet content providers. According to the Chinses legislature history, the laws and

[98] *See* RPRD, art. 14-17.
[99] 2014 Copyright Draft, *supra* note 30, art. 73 para. 1.
[100] 2014 Copyright Draft, *supra* note 30, art. 73, para. 2.

regulations have stipulated related provisions on Internet content services, therefore, it is unnecessary to stipulate again in the E-commerce Law.

However, it is arguable to exclude online content services from E-commerce Law because: (1) online content services is part of the e-commerce; (2) massive online copyright infringement issues still exist in China; and (3) Article 41 of the E-commerce Law promotes IPRs protection in all IP regimes including copyright. Moreover, the RPRD that stipulates relevant provisions of online content services is a regulation, not a law. Furthermore, the Third Amendment of the Copyright Law is still under deliberation. As a result, E-commerce Law defines ISPs in a broad way, but does not cover Internet content providers, which means most of the online copyright issues of ISPs are not covered in the E-commerce Law.

Although E-commerce Law does not cover Internet content providers, defining ISPs in a broad way is a significant improvement on IPR protection of ISPs in China. Starting from January 1st, 2019, all the ISPs except Internet content providers will be regulated under the E-commerce Law. As Yin Zhongqing, the vice chairman of Financial Affairs Committee, said at a press conference held by the General Office of the NPC Standing Committee after the E-commerce Law was promulgated, "the law … covers not only famous platforms such as Alibaba's Taobao but also those selling goods via social networks including the popular social media app WeChat."[101] So far, the 2010 Copyright Law and the RPRD regulates Internet content providers. Other than that, all the IPRs issues relating to ISPs shall be regulated by the E-commerce Law.

In sum, E-commerce law adopts an active-preventive approach of ISPs by putting more emphasis on the obligations and responsibilities held by platform operators, who are the most

[101] Yan, *China Focus: China adopts e-commerce law to improve market regulation*, Xinhua (新华网), (Aug. 31, 2018 23:07) Available at: http://www.xinhuanet.com/english/2018-08/31/c_137434452.htm (last visited Sep. 23, 2018).

advantaged players in the country's e-commerce market.[102] Moreover, it also strengthens protection for the relatively disadvantaged consumers, who are the biggest victims of IP infringement.[103] Although relevant provisions regarding specific IP issues still exist in different laws and regulations, the E-commerce Law sets up a unified IP protection system that constitutes a legal foundation for ISPs to prevent IP infringements.

[102] NPC Standing Committee (全国人大常委会), *Press conference of the General Office of the NPC Standing Committee (2018.08.31)* (全国人大常委会办公厅 2018 年 8 月 31 日新闻发布会). Available at http://www.npc.gov.cn/npc/zhibo/zzzb36/node_27366.htm (last visited Sep. 23, 2018).
[103] Yan, *supra* note 101.

Chapter III: Secondary Copyright Liability of ISPs

Online copyright infringement occurs when a third party violates one or more of the copyright owner's exclusive rights through information networks. As intermediaries, ISPs are liable for secondary copyright infringements even though it is the Internet users who directly infringe copyright by the services of ISPs. Before examining the impact of the E-commerce Law to the copyright liability of ISPs in China, this chapter reviews the recent development of secondary copyright liability of ISPs in the U.S. and China, and then examines different approaches to the secondary copyright liability issue of ISPs through a comparative methodology.

This chapter contains three parts. Part A introduces the development of secondary liability theory in the U.S. as a background before analyzing cases of ISPs. The ISPs statutes and cases in the U.S. will be compared to the Chinese statutes and cases of in Part B. Part A Section 1 presents the historical background of the copyright infringement theories of ISPs. Section 2 analyzes potential legal defense for copyright liability of ISPs under U.S. law. Section 3 examines several copyright infringement cases of ISPs in recent years.

Part B demonstrates the development of secondary copyright liability of ISPs in China by comparing the statutes and cases of ISPs in the U.S. Section 1 introduces the liabilities of ISPs under Chinese laws and regulations before the E-commerce Law. Section 2 presents the background of the E-commerce Law and analyzes the impact of the E-commerce Law to ISPs on China.

Part C presents several recent cases of ISPs in China. Section 1 and Section 2 analyze two cases of secondary copyright liability issues and compare them with the cases in the U.S. Section 3 compares the different approaches on the issue of unauthorized third-party software between China and the U.S.

A. Secondary copyright liability of ISPs in the U.S.

Before the digital age, the secondary copyright liability theory had been developed in the law of torts in the U.S. Additionally, the legislature enacted the DMCA in 1998 for the new copyright challenge introduced by the digital world. The DMCA was "designed to facilitate the robust development and world-wide expansion of electronic commerce, communications, research, development, and education."[104] To balance the interest between the Internet users, ISPs and the copyright owners, the DMCA built one of the earliest models of ISPs with two major theories: the safe harbor doctrine and the N&T policy. As new copyright issues arose 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 influenced other jurisdictions such as China. Therefore, before discussing the copyright liability of ISPs in China, it is necessary to review the development of secondary liability of ISPs in the U.S.

Section 1 begins with an overview of the development of secondary liability of ISPs in the U.S. Section 2 examines the copyright liability theories of ISPs through the DMCA statutes and the potential defense of ISPs. Based on these two sections, Section 3 examines five recent ISP cases to (1) demonstrate the U.S approach on how the courts applied laws of ISPs to solve online copyright disputes; and (2) provide the case law background of ISPs, which will be compared to the Chinese ISPs cases in Part B.

1. Background

In the digital era, anyone who has access to the Internet can easily acquire copyright works in digital forms. Internet users can download or make multiple copies of an original work and distribute the digital copy of the work on the Internet. As intermediaries, ISPs provide

[104] S. REP. No. 105-190, at 1-2 (1998).

perfect platforms for Internet users to find these digital works by the strong searching and linking capabilities of network technology.[105] As a result, these Internet users may easily infringe copyright work as long as their activities are not authorized by copyright owners.

The legal issues raise by ISPs infringement are contentious today. The scenario is easy: individual infringers of unauthorized work are obviously guilty of copyright infringement. However, whether the firms and individuals that owned implicated ISPs are also liable is controversial. From one perspective, because ISPs have done nothing more than intermediaries where Internet users can use their technologies and services, ISPs should not be liable for the infringing activities of their users or subscribers. However, ISPs benefit from infringement because infringing copyright work is part of what brings Internet users to the ISPs. Moreover, ISPs are likely able to do more to crack down on unlawful behavior, such as implanting filter technology or blocking infringers' online accounts.

Nonetheless, because of the anonymity of the Internet, these Internet users who directly infringe copyright online are difficult to track or locate. Moreover, individuals who are skilled in digital technology can easily revise, modify, and adapt copyright works by using different technological tools. Therefore, it is almost impossible for the copyright owners to confirm and sue all the direct infringers. For example, tracking a network user is hard if the user uses a virtual private network (VPN). Because a VPN can show a different Internet Protocol address (IP address) instead of the real IP address of the electronic device, tracking a VPN user could be extremely expensive and time-consuming. As a result, copyright owners tend to make actions against intermediaries, such as ISPs, who provide the platform to their users and subscribers. Although the ISPs seldom copy or distribute copyrighted works directly, the technologies and devices they provide may facilitate the direct infringers, and therefore, they

[105] JERRY JIE HUA, TOWARD A MORE BALANCED APPROACH: RETHINKING AND READJUSTING COPYRIGHT SYSTEM IN THE DIGITAL NETWORK ERA, 101 (Springer 2014).

may be responsible for secondary copyright infringement liability. As a result, how the legal interests among the Internet users, ISPs and copyright owners should be balanced is a controversial issue.

a. Legal theories of the copyright infringement liability of ISPs in the U.S.

As Justice Scalia, J concluded in *Aereo*[106]: "There are two types of liability for copyright infringement: direct and secondary … Most suits against equipment manufacturers and service providers involve secondary-liability claims."[107] This section introduces the legal theories of the copyright infringement liability of ISPs, with a special focus on the secondary infringement liability of ISPs.

i. Liability of direct copyright infringement

Section 501(a) of the 1976 Copyright Act provides that: "anyone who violates any of the exclusive rights of the copyright owner … is an infringer of the copyright."[108] In other words, when a third party violates one or more of the copyright owner's exclusive rights mentioned in the 1976 Copyright Act,[109] the violator infringes copyright, and therefore, bear copyright liability. For example, anyone who copies the original work without the author's authorization is considered as a direct infringer. In order to sustain an action for infringement, the copyright owner must prove three things: (1) the ownership of a valid copyright for the work; (2) that the work was copied by the defendant; (3) that the defendant's copying constitutes an improper appropriation.[110] However, proving infringement of a direct infringer can be difficult in digital world.

For example, anyone who knows how to use electronic devices can easily make copies

[106] American Broadcasting Crop. v. Aereo, 134 S. Ct. 2498 (2014).
[107] *Id.* at 2512 (Scalia, J., dissenting).
[108] 17 U.S.C.§ 501(a).
[109] 17 U.S.C.§ 106.
[110] MARSHALL A. LEAFFER, UNDERSTANDING COPYRIGHT LAW 419 (LexisNexis 5th ed. 2010).

of the original work and distribute them through Internet. Thus, it could be expensive and time-consuming for copyright owners to track individuals who directly infringed on their copyright. Therefore, proving direct copyright infringement could be extremely costly for the copyright owner in this case.

On the other hand, ISPs are much easier to be targeted by the copyright owners. Because most ISPs provide services to the public, copyright owners can easily pinpoint the ISPs when they discover the infringing activities on the ISPs' websites. As mentioned before, liability of direct copyright infringement apples when a third party personally engages in infringing conduct.[111] Therefore, ISPs shall bear direct copyright infringement liability if they directly engage with infringing activities. However, whether ISPs shall bear copyright infringement liability if their users or subscribers engage with infringing activities on their services is questionable. This section discusses whether ISPs should bear copyright infringement liability because of facilitating direct infringers as intermediaries below.

ii. Liability of secondary copyright infringement

If ISPs provide copyrighted work on their platforms to the public without authorization by copyright owners, they can be liable for direct copyright 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 ISPs may have no actual knowledge of what their users did, they can be held liable for actively aiding another to infringe copyright.[112] While the 1976 Copyright Act does not expressly impose liability on anyone other than direct infringers, courts have recognized that vicarious or contributory liability can

[111] *See* Sony Corporation of America v. Universal City Studios Inc., 104 S. Ct. 774, 784 (1984).
[112] LEAFFER, *supra* note 110, at 438.

be imposed in certain circumstances.[113]

(1). Contributory Liability

The contributory infringement doctrine originated in tort law and stemmed from the principle that one party knowingly induces, causes, or otherwise materially contributes to the infringing conduct of another.[114] 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.[115] To establish a contributory liability claim against an ISP, 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; and (3) the ISP should have caused or materially contributed to the underlying direct infringement.[116]

(2). Vicarious Liability

Vicarious liability applies where one party has control over another and enjoys a direct financial benefit from that other's infringing activities.[117] Unlike contributory infringement, under the 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. To establish a vicarious liability claim against an ISP, a copyright owner needs to prove that: (1) there is a direct infringement by a primary infringer; (2) the ISP has the right and ability to control or supervise the underlying direct infringement; and (3) the ISP derived a direct financial benefit from the underlying direct infringement.[118]

---

[113] *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).
[114] Douglas Lichtman & William Landes, *Indirect Liability for Copyright Infringement: An Economic Perspective*, 16 HARV. J. L. & TECH. 395, 396 (2003).
[115] Fonovisa, Inc. v. Cherry Auction, Inc., 76 F.3d 259, 264 (9th Cir. 1996).
[116] Parker v. Google, Inc., 242 Fed.Appx. 833, 837 (3d Cir.2007).
[117] Douglas Lichtman & William Landes, *supra* note 114, at 398.
[118] Gershwin Publishing Corp. v. Columbia Artists Management, Inc., 443 F.2d 1159, 1162 (2d Cir.1971).

iii. *Sony*'s "staple article" rule

Before the DMCA was enacted in 1998, *Sony Corp. v. Universal City Studios Inc.*[119] was an influential case that established a safe harbor system for technological intermediaries. The issue was whether Sony's product, Betamax video cassette recorder (VRC), indirectly infringed Universal's copyright. VRC was an innovative product that could be used both for legal time-shifting purpose and unlawful purpose of copyright infringement. The U.S. Supreme Court adopted neither the contributory infringement theory nor the vicarious liability theory, but borrowed a staple article of commerce doctrine from the U.S. Patent Law[120] and concluded that "the sale of a 'staple article or commodity of commerce suitable for substantial noninfringing use' is not contributory infringement."[121] As a result, the court held that the VRC was capable of substantial noninfringing use and therefore could not be banned.

The *Sony* "staple article" rule creates a balance between copyright owners' demand for effective protection and the rights of others, such as ISPs, to engage in substantially unrelated areas of commerce.[122] After *Sony*, even though some users or subscribers will predictably use the technologies of ISPs to infringe copyright, the secondary copyright infringement liability of ISPs was limited. As a result, the *Sony* rule influenced the development of online copyright infringement theory for ISPs by creating opportunities to new online technology and business.

iv. Active inducement rule

After the safe harbor doctrine was enacted in the DMCA, the U.S. Supreme Court interpreted the *Sony* rule in *MGM v. Grokster*.[123] The Court analyzed the holding in *Sony* and the staple article of commerce doctrine from patent law, and concluded that the Court of

[119] *Sony Corp. of Am. v. Universal City Studios Inc.*, 104 S. Ct. 774 (1984).
[120] *See* 35 U.S.C. § 271(c).
[121] *Sony*, 104 S. Ct. at 788.
[122] *Id.*
[123] Metro-Goldwyn-Mayer Studios Inc. v. Grokster Ltd., 125 S. Ct. 2764 (2005).

Appeals misunderstood *Sony* rule because "*Sony*'s staple-article rule will not preclude liability."[124] After citing several cases 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."[125] Based on the court's decision, the active inducement rule requires that: (1) the ISP has actual knowledge of infringing conduct; and (2) the ISP had an affirmative intent or step to incite direct copyright infringement.

Under the active inducement rule, even if ISPs can show substantial noninfringing use of their technology, they will be held secondary copyright infringement liability for actively inducing their users or subscribers to infringe copyright. In conclusion, the secondary copyright liability theory of ISPs develops with technology progress and business, and keep creating balance among the copyright owners, ISPs and public interest.

2. ISPs' potential defense in the U.S.

This section introduces the ISPs' potential defenses under the 1976 Copyright Act, which provides a background before analyzing cases of ISPs in Section 3. Whenever the copyright owners discover copyright infringement on ISPs, they have to prove: (1) the ownership of their copyright on the infringing material, and (2) the direct or indirect infringers violated at least one of their exclusive rights. Because ISPs usually infringes copyright indirectly as intermediaries, this section focuses on the potential defense for the secondary copyright infringement.

a. Potential defense for direct copyright infringement of ISPs

The U.S. Copyright Act provides six exclusive rights for copyright owners, and the

[124] *Grokster*, 125 S. Ct., at 2779.
[125] *Id.* at 2780.

violation of any of those rights constitutes copyright infringement. Each exclusive right is subject to a series of limitations, such as the fair use doctrine in Section 107. Even though the copyright owners can prove their ownership of the copyright, the ISPs can counterclaim that they did not infringes the exclusive rights of copyright owners based on the limitations of these rights. Because these limitations are complex, courts usually apply these limitations issues on a case by case basis. This section will examine one of the limitations under the Family Movie Act of 2005 (FMA)[126] through a case in Section 3.

b. Potential defense for secondary copyright infringement of ISPs

i. Safe harbor doctrine and the N&T provision

The DMCA establishes a safe harbor doctrine[127] for ISPs and its purpose is to provide a balance between protecting copyright holders and ISPs' liability. In order to be protected by the safe harbor doctrine from direct or secondary copyright liability, ISPs must follow the N&T provision.[128] The N&T provision requires copyright owners to send a proper notification to ISPs when they discover infringing material on an ISP platform. Upon receiving notification, the ISP must promptly remove or block access to the alleged material in order to obtain immunity from copyright liability.

These two core principles from the DMCA are influential and most other jurisdictions adopts a similar safe harbor doctrine and N&T provisions in their copyright laws, such as China. These two traditional principles are considered as a passive-reactive approach to the liability of ISPs. This approach requires ISPs to act passively regarding copyright protection until the copyright owners send notification regarding copyright infringement. The ISPs should react according to the notification in order to obtain protection provided by the safe harbor. Thus, a

[126] 17 U.S.C. § 110(11).
[127] 17 U.S.C.§ 512.
[128] 17 U.S.C. § 512(c)(1), *See also* 17 U.S.C. § 512 (d).

traditional passive-reactive ISP approach requires ISPs to act passively and neutrally.[129]

A critical opinion on a passive-reactive ISP approach is that ISPs have no incentive to protect copyright on their platforms. It is likely that ISPs may abuse the safe harbor defense to avoid copyright infringement. To promote online IP protection, an active-preventive approach of ISPs is raised by the U.S. courts and some jurisdictions. This Section examines an active-preventive approach to ISPs from the Second Circuit in *Viacom Intern., Inc v. Google/YouTube Inc.*,[130] which will be compared to the active-preventive approach of ISPs in China in Part B.

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

It is possible that ISPs could be contributory or vicarious liable for their users' infringing activities, even though these copyright infringements are unknown to the ISPs. In order to limit ISPs' liability from copyright infringement, OCILLA (known as the "safe harbor provision") was passed as Title II of the 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; and (4) information location tools.[131] When ISPs' activities qualify in one of the categories, they are exempted from copyright liability.

In order to trigger any of the exemptions from the safe harbor provisions, an ISP must meet two threshold conditions in Section 512(i): (1) a service provider must adopt, implement, and inform its users of its policy that provides termination of users who are repeated infringers;[132] and (2) The ISP must accommodate and not interfere with standard technical measures that are used by copyright owners to identify and protect copyrighted works.[133] However, merely implementing policy and technical measures may not be enough because

[129] JEREMY & CHRISTOPHER, *supra* note 2, at 377.
[130] *Viacom Int'l, Inc. v. YouTube, Inc.*, 676 F.3d 19 (2d Cir. 2012).
[131] 17 U.S.C. § 512(a)-(d).
[132] 17 U.S.C. § 512(i)(1)(A).
[133] 17 U.S.C. § 512(i)(1)(B).

courts may "require[s] something more than the ability to remove or block access to materials posted on a service provider's website."[134] The *YouTube* case in Section C discusses this "something more" standard in depth.

iii. Section 512(c)-(d)

In addition to the general provisions from Section 512(i), Section 512(c) and (d) may immunize the ISPs 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 that: (1) the ISP does not have actual knowledge or awareness of facts or circumstances from which infringing activity is apparent;[135] (2) the ISP does not receive financial benefits directly from the infringing activity, in a case in which the service provider has the right and ability to control such activity;[136] and (3) the ISP 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.[137] Such provisions provide ISPs, especially Internet content providers, a safe harbor to avoid secondary infringement liability of their users.

However, even though China also adopted similar provisions in its mechanism of ISPs before the E-commerce Law, it did not effectively prevent online copyright infringement. Thus, to promote online copyright protection, the Chinese legislation plans to adopt an active-preventive approach of ISPs by excluding Internet content providers from safe harbor provisions.[138] Part B analyzes this approach in depth.

---

[134] *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).
[135] 17 U.S.C. § 512(c)(1) & § 512(d)(1).
[136] 17 U.S.C. § 512(c)(2) & § 512(d)(2).
[137] 17 U.S.C. § 512(c)(3) & § 512(d)(3).
[138] *See* 2014 Copyright Draft, *supra* note 30, art. 73 para. 1 & para. 5.

c. Potential defense under anticircumvention provision

With the development of digital technology, copyright owners can adopt multiple technological protection measures (TPMs) to prevent their digital works from infringement. Article 11 of the WCT requires its members to provide adequate legal protection and remedies against the circumvention of TPMs.[139] The U.S. Congress conformed WCT requirements in the DMCA with and enacted them in Section 1201 of the Copyright Act, which prohibits the conduct of circumvention and manufacture or trafficking of technologies that are designed to circumvent TPMs.[140]

Section 1201 contains three new causes of action for copyright owners to prohibit circumvention of TPMs: Section 1201(a)(1) is a general prohibition against circumventing TPMs that control access to a copyrighted work.[141] Section 1201(a)(2) prohibits trafficking in technology that facilitates circumvention of such access-control TPM to a copyrighted work.[142] Section 1201(b)(1) prohibits trafficking in technology that facilitates circumvention of copy-protection TPMs to copyright owners' rights. Since the interrelationship of these provisions are complex, next paragraph presents an example to explain the difference among these provisions.

For instance, copyright owners adopt a digital lock as a TPM to access their copyrighted work in a Portable Document Format (PDF). They also adopt a technology that prevent PDF files from copying or editing. To open the digital lock and access the content in the PDF, the users must subscribe to the copyright owners in order to acquire a password. However, some users choose to purchase a software that can bypass the digital lock. Moreover, the provider of the software also sells a circumventing technology that allow users to copy or edit the PDF. For this hypothetical case, Section 1201(a)(1) prohibit against any users who use a software to

[139] WIPO Copyright Treaty, art. 11.
[140] LEAFFER, *supra* note 110, at 406.
[141] 17 U.S.C. § 1201(a)(1).
[142] 17 U.S.C. § 1201(a)(2).

bypass the digital lock; Section 1201(a)(2) prohibit against anyone who provide a software to bypass the digital lock; Section 1201(b)(1) prohibit against anyone who provide a circumventing technology to infringe copyrighted work in the PDF.

Because the act of circumvention is an independent violation that does not affect defenses to copyright infringement,[143] the violator who circumvents the TPMs is separately liable under Section 1201. In other words, circumvent liability and copyright infringement liability are separate in the Copyright Act. In addition, the prohibitions contained in Section 1201 are subject to a number of exceptions, which can be used as defenses against anticircumvention claims. To explain these complex anticircumvention provisions, this chapter will analyze Section 1201 on a case by case basis, especially the *Blizzard* case and the *VidAngel* case in the Section 3.

3. Cases of ISPs in the U.S.

This section analyzes four cases that involve copyright infringement liability of ISPs to conclude how the courts apply laws of ISPs in the U.S. The ruling from these cases will also be compared to Chinese laws in Part B and cases of ISPs in Part C, so as to demonstrate the similarities and differences of the issues of ISPs between the U.S. and China. First, the *Aereo* case addressed a new issue about online retransmission, which raised a debatable question on whether secondary transmission of ISPs infringes copyright owner's exclusive rights. Second, in the *VidAngel* case, the defendant tried to use the Supreme Court's opinion in *Aereo* and the Family Movie Act of 2005 (FMA)[144] as a defense to avoid copyright infringement liability. Part C compares these two cases with the *SOHO* case in order to conclude the differences on secondary retransmission issues of ISPs between the U.S. and China.

Third, in the *Blizzard* case,[145] the Ninth Circuit overturned the district court's decision

[143] 17 U.S.C. § 1201(c)(1).
[144] 17 U.S.C. § 110(11).
[145] *MDY Industries, LLC. v. Blizzard Entertainment, Inc.*, 629 F.3d 928 (2011).

on secondary infringement of unauthorized third-party software, and ruled that there is a violation of Section 1201(a)(2) of the DMCA. Part C compares *Blizzard* with the *Qihoo Tech Ltd. (Beijing) v. Tencent Tech Ltd. (Shenzhen)* (hereinafter "*Tencent*")[146] case in order to show why the Chinese software owners tend to use unfair competition law instead of copyright law to tackle unauthorized third-party software.

Fourth, 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 subjective and objective standard, and the "something more" doctrine. Part C compares *YouTube* with the *Beijing China Youth Publishing Group v. Beijing Baidu Tech Ltd.* (hereinafter "*Baidu*") case[147] to show how the Beijing High People's court applied a similar rationale in *YouTube* on the issues of secondary copyright infringement.

a. American Broadcasting Cos., Inc. v. Aereo, Inc.

ABC v. Aereo[148] is one of the most recent cases involving ISPs from the U.S. Supreme Court. The defendant Aereo, Inc. captured and transcoded over-the-air broadcast television programming signals by its miniature antenna per every customer, and then retransmitted 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."[149] Different from other ISP copyright infringement cases, the plaintiffs, American

---

[146] Bei jing qi hu ke ji you xian gong si, qi zhi ruan jian (bei jing) you xian gong si yu teng xun ke ji (shen zhen) you xian gong si, shen zhen shi teng xun ji suan ji xi tong you xian gong sib u zheng dang jing zhen jiu feng an er shen min shi pan jue shu [北京奇虎科技有限公司、奇智软件（北京）有限公司与腾讯科技（深圳）有限公司、深圳市腾讯计算机系统有限公司不正当竞争纠纷案二审民事判决书 [Qihoo Tech Ltd. (Beijing) v. Tencent Tech Ltd. (Shenzhen)], [Sup. People's Ct. (中华人民共和国最高人民法院) Feb 18, 2014], (2013) Min San Zhong Zi No. 5 [(2013) 民三终字第 5 号] (China) [hereinafter *Tencent*].

[147] Bei jing Zhong qiang wen wen hua chuan mei you xian gong si deng zhu zuo quan quan shu, qing quan jiu fen ger shen ming shi pan jue shu (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) [Beijing China Youth Publishing Group v. Beijing Baidu Tech Ltd.], [Beijing High People's Ct. (北京市高级人民法院) Aug 5, 2014], 2014 Gao Min Zhong Zi No. 2045 [(2014) 高民终字第 2045 号)] [hereinafter *Baidu*].

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

[149] *Id.* at 2503.

Broadcasting Companies, Inc. (hereinafter "ABC"), focused their claim on direct infringement of one of the copyright owner's exclusive right: public performance right.[150] 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 was unclear. Therefore, the issues in this case were whether Aereo (1) operated an automated, user-controlled system and infringed plaintiffs' public performance right; and (2) was liable for retransmitting copyrighted performance and reproduction.

i. Public performance right

For the first issue, the majority of the court considered Aereo as a community antenna television (CATV) company. The majority 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 'perform[s]'."[151] For the second issue, the court referred to Section 111 of the 1976 Copyright Act that governs cable television system. 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…"[152] and "a 'secondary transmission' is the further transmitting of a primary transmission simultaneously… or nonsimultaneously with the primary transmission…"[153] The question is whether Aereo's secondary transmission of ABC's primary transmission should be considered a public performance. As a result, the court held that "Aereo transmits a performance of petitioners copyrighted works to the public, within the meaning of the Transmit Clause."[154]

---

[150] 17 U.S.C. § 106(4).
[151] *Aereo,* 134 S. Ct. at 2507.
[152] 17 U.S.C. § 101(f)(1).
[153] 17 U.S.C. § 101(f)(2).
[154] *Aereo,* 134 S. Ct. at 2510.

ii. Retransmission right

Although Aereo provided online retransmit services, the court recognized Aereo as CATV and did not expand its ruling to ISPs. On the contrary, the court concluded a limited holding and emphasized that it did not intend to discourage the emergence and use of new technology, such as cloud. For example, if a user lawfully downloads a movie and uploads it to the cloud, when the user decides to watch the movie from it, the ISP that provides cloud service will stream the movie from its server to its user. Although the ISP stores and streams the movie via its server, it does not violate the public performance right because (1) the user owns the movie; and (2) the user screens the movie. As a result, the court construed that "the term 'the public' … does not extend to those who act as owners or possessors of the relevant product" and "[are] 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."[155]

However, the rationale of this limited holding is not perfect and creates a loophole in copyright law. On one hand, the rationale of the court seems correct because the ruling of this case can be problematic if it were to apply to all ISPs, 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 a "secondary transmitter," and therefore, performing copyrighted work to the public. On the other hand, the scope of this case is too narrow, and therefore it can not apply to other secondary transmission issues of ISPs, such as live streaming or video on-demand. An online streaming user can easily retransmit a copyrighted work without the authorization of the copyright owner. Moreover, if an online streaming user lawfully acquires a copyrighted work, whether

[155] *Aereo*, 134 S. Ct. at 2510-2511.

retransmitting a copyright work online infringes copyright owner's exclusive rights is questionable. Although *Aereo* did not clarify this issue, a recent case from the Ninth Circuit Court of Appeals has addressed this issue on whether reforming and streaming a lawfully purchased copyright work infringes a copyright owner's exclusive rights, which will be discussed below.

b. Disney Enterprises, Inc. v. VidAngel, Inc.

In the *Disney v. VidAngel* case (hereinafter "*VidAngel II*"),[156] the defendant VidAngel, Inc. lawfully purchased copyrighted movies and television shows on physical discs, and decrypted them to digital copies in order to remove objectionable content from movies and television shows. The defendant stored filtered versions of these copyrighted works in the cloud server and retransmitted them to its subscribers through online streaming service. "VidAngel was not licensed or otherwise authorized to copy, perform, or access any of these works."[157] The plaintiffs, Disney Enterprises and other Studios (hereinafter "Studios"), alleged copyright infringement on their exclusive rights of public performance and reproduction,[158] and circumvention of technical measures.[159] The defendant raised defense from *Aereo* and FMA that "the was designed to allow consumers to skip objectionable audio and video content in motion pictures without committing copyright infringement."[160]

i. Public performance right

Although the Court of Appeals did not explain the issue of public performance right, in *VidAngel I*,[161] the defendant cited *Aereo* in the district court and argued that its streaming service did not engage in public performance because its subscribers paid and owned filtered

[156] *Disney Enterprises, Inc. v. VidAngel, Inc.*, 869 F.3d 848 (2017) [hereinafter *VidAngel II*].
[157] *VidAngel II*, 869 F.3d at 855.
[158] 17 U.S.C. § 106(1) & (4).
[159] 17 U.S.C. § 1201(a)(1)(A).
[160] *VidAngel II*, 869 F.3d at 857.
[161] *Disney Enterprises, Inc. v. VidAngel, Inc.*, 224 F. Supp. 3d 957 [hereinafter *VidAngel I*].

versions of motion pictures.[162] Under *Aereo,* a transmission of a copyrighted program is not made to "the public" when it is made "to those who act as owners or possessors of the relevant product."[163] However, the district court rejected the defendant's defense by ruling that "lawful ownership of a DVD only conveys authorization to view the DVD, not to decrypt it for the purpose of viewing it on an alternative platform."[164] As a result, the district court found that VidAngel violated plaintiffs' exclusive rights and defendant appealed with two issues: (1) whether the FMA[165] of 2005 exempts VidAngel from liability for copyright infringement; and (2) whether the anti-circumvention provision of the DMCA covers the plaintiffs' technological protection measures (TPMs), which control both access to and use of copyrighted works.[166]

ii. FMA

On the first issue, the court of appeal agreed with district court's decision that VidAngel infringed reproduction right of plaintiffs by copying copyrighted works from discs onto a computer. According to Section 109 of the Copyright Act, even though VidAngel was a lawful owner "of a particular copy,"[167] it was "only entitled to 'sell or otherwise dispose of the possession of that copy,' not to reproduce the work."[168] Therefore, VidAngel also infringed public performance right of plaintiffs because the subscribers of VidAngel paid for the digital content streamed to them, not for the physical discs. Nonetheless, the defendant brought up the FMA defense and argued that its filtered streaming was authorized because the streaming

[162] *VidAngel I*, 224 F. Supp. 3d, at 970.
[163] *VidAngel I*, 224 F. Supp. 3d, at 971. Citing *Aereo*, 134 S. Ct. at 2510.
[164] *Id*.
[165] 17 U.S.C. § 110(11): Notwithstanding the provisions of section 106, the following are not infringements of copyright: … (11)the making imperceptible, by or at the direction of a member of a private household, of limited portions of audio or video content of a motion picture, during a performance in or transmitted to that household for private home viewing, from an authorized copy of the motion picture, or the creation or provision of a computer program or other technology that enables such making imperceptible and that is designed and marketed to be used, at the direction of a member of a private household, for such making imperceptible, if no fixed copy of the altered version of the motion picture is created by such computer program or other technology.
[166] *VidAngel II*, at 852.
[167] 17 U.S.C. § 109(a).
[168] *VidAngel II*, at 856.

originated from an authorized copy. The court rejected this defense by saying that VidAngel's filter process did not meet the "imperceptible" requirement in Section 110(11) because no fixed copy of the altered version of the motion picture could be created, and concluded that "VidAngel's interpretation would create a giant loophole in copyright law, sanctioning infringement so long as it filters some content and a copy of the work was lawfully purchased at some point."[169] As a result, VidAngel was liable for infringing Studios' exclusive rights under Section 106.

iii. Section 1201(a)(1)

The second issue concerns whether VidAngel was liable for the circumvention liability under Section 1201(a)(1), the defendant argued that because the discs were lawfully purchased, it was authorized by the Studios to decrypt the TPMs to view the discs' content. The court rejected this argument by citing *Blizzard* that although Section 1201(a)(3)(A)[170] exempts those "whom a copyright owner authorizes to circumvent an access control measure [from circumvention liability], not those whom a copyright owner authorizes to access the work."[171] Therefore, "lawful purchasers have permission only to view their purchased discs with a DVD or Blu-ray player licensed to decrypt the TPMs."[172] Moreover, the court also clarified that "when a defendant decrypts the TPMs and then also reproduces that work, it is liable for both circumvention in violation of § 1201(a)(1)(A) and copyright infringement in violation of § 106(1)."[173] As a result, the court agreed with the district court's decision that VidAngel decrypted the access controls on the plaintiff's discs without authorization, and therefore, was liable under Section 1201(a)(1).

---

169 *VidAngel II*, at 859.
170 17 U.S.C. § 1201(a)(3)(A): "To 'circumvent a technological measure' means to descramble a scrambled work, to decrypt an encrypted work, or otherwise to avoid, bypass, remove, deactivate, or impair a technological measure, without the authority of the copyright owner."
171 *MDY Indus., LLC. v. Blizzard Entm't, Inc.*, 629 F. 3d, 928, 953 n. 16 (9th Cir 2011).
172 *VidAngel II*, at 863.
173 *VidAngel II*, at 864.

The court did not analyze whether the defendant's decryption technology violates Section 1201(a)(2) and Section 1201(b)(1). These two anticircumvention provisions will be discussed in the *Blizzard* case below.

c. MDY Industry, LLC. V. Blizzard Entertainment, Inc.

i. Background

Whether unauthorized third-party programs such as cheat, bot or plugin constitute copyright infringement is a serious issue in game industry. In the *Blizzard* case (hereinafter "*Blizzard I*"[174] & "*Blizzard II*"[175]), the defendant Blizzard Entertainment, Inc (hereinafter "Blizzard") is a famous video game company that created many popular games. One of Blizzard's popular games, World of Warcraft (WoW), is a multiplayer online role-playing game that allows players interact in a virtual world. The WoW players can roleplay multiple characters in the game and their characters may advance to higher levels for more virtual currency, stronger abilities and better equipment. In March 2005, Plaintiff MDY Industries, LLC. (hereinafter "MDY") and its sole member Michael Donnelly (hereinafter "Donnelly") developed and sold Glider, a software program that automatically plays WoW for players. Blizzard recognized Glider as a bot that performs the same operation many times in a row. It also believed that Glider enabled their users to quickly advance levels and unfairly gain game assets.

In September 2005, Blizzard launched Warden, a software that detect and block unauthorized third-party software including Glider. In November 2005, MDY responded by offering anti-detection software Glider Elite and filed a complaint seeking a declaration that Glider does not infringe Blizzard's copyright or other rights on WoW. Blizzard filed counterclaims and third-party claims against MDY for, inter alia, contributory and vicarious

[174] MDY Indus., LLC. v. Blizzard Entm't, Inc., 616 F. Supp. 2d, 958 [hereinafter *Blizzard I*].
[175] MDY Indus., LLC. v. Blizzard Entm't, Inc., 629 F. 3d, 928 [hereinafter *Blizzard II*].

copyright infringement, violation of DMCA Section 1201(a)(2) and (b)(1), and tortious interference with contract. This case analyzes the secondary copyright infringement issue and the Section 1201 issue, and concludes a proposal for game industry against unauthorized third-party program.

ii. Secondary infringement

The existence of direct copyright is a prerequisite to prove secondary copyright infringement. However, In *Blizzard I*, the district court adopted a two-prong test to determine whether Donnelly was secondarily liable for copyright infringement, and held that "Donnelly clearly supervised the infringing and circumventing activities of MDY and profited personally from their success… Donnelly is liable for MDY's vicarious copyright infringement, contributory copyright infringement, and DMCA violations."[176] The findings appear to meet multiple prerequisites for secondary infringement such as: (1) Donnelly had actual knowledge that Gilder users cheated in WoW; (2) Donnelly had the right and ability to supervise the Gilder; (3) Donnelly had a direct financial interest in selling Glider; and (4) Donnelly induced WoW players to use Gilder. Nonetheless, the district court did not analyze whether the WoW players who use Glider committed direct copyright infringement, which is fundamental prerequisite for committing a secondary copyright infringement.

In *Blizzard II*, the court of appeals reversed the district court's decision on secondary copyright infringement, and concluded that "WoW players do not commit copyright infringement by using Glider ... MDY is thus not liable for secondary copyright infringement, which requires the existence of direct copyright infringement."[177] On determining whether WoW players committed direct copyright infringement by using Glider, the court first analyzed whether WoW players, including Glider users, infringed Blizzard's exclusive rights of WoW

[176] *Blizzard I*, 616 F. Supp. 2d, at 973.
[177] *Blizzard II*, 629 F. 3d, at 941.

software. Second, the court considered whether WoW players were owners or licensees of their copies of WoW software, which is a copyright issue on software.

When playing WoW, a player's computer creates a copy of the game's software in the computer's random access memory (RAM),[178] therefore, potentially infringing Blizzard's reproduction right on WoW. If a WoW player owns the copy of the software, the player could claim "essential step" defense under Section 117(a)(1)[179] of the Copyright Act. To run a software, a computer copies the software files from its hard drive to its RAM, which may potentially infringe the software owner's reproduction right. Section 117(a)(1) provides limitations on exclusive rights of computer programs so that software users will not infringe reproduction right when using software on their personal device. Because copying WoW software in RAM is an "essential step" for Glider users to play WoW on their computers, thus, Glider users do not directly infringe Blizzard's reproduction right, and MDY is not secondarily liable for copyright infringement.

However, the court adopted a test from *Vernor v. Autodesk*[180] and held that WoW players were licensees of WoW's software and did not own the copies of WoW.[181] In *Vernor*, on determining whether a software user is a licensee rather than an owner of a copy, the Ninth Circuit of Appeals considered whether the copyright owner (1) specifies that the user is granted a license; (2) significantly restricts the user's ability to transfer the software; and (3) imposes notable use restrictions.[182] Because WoW players must read and accept Blizzard's End User License Agreement (EULA) and Terms of Use (ToU) before playing, the court held that WoW players, including Glider users, were granted non-exclusive, limited license by Blizzard.[183]

---

[178] RAM is a form of temporary memory used by computers to run software programs.
[179] 17 U.S.C. § 117(a)(1): "Notwithstanding the provisions of section 106, it is not an infringement for the owner of a copy of a computer program to make or authorize the making of another copy or adaptation of that computer program provided: (1) that such a new copy or adaptation is created as an essential step in the utilization of the computer program in conjunction with a machine and that it is used in no other manner."
[180] *Vernor v. Autodesk, Inc.*, 621 F.3d 1102 (9th Cir. 2010).
[181] *Blizzard II*, at 938.
[182] *Vernor*, 621 F.3d, at 1110-1111.
[183] *Blizzard II*, at 938.

A licensee can be sued for direct copyright infringement if the licensee (1) acts outside the scope of the license; and (2) such action implicates licensor's exclusive rights.[184] Although a WoW player who used Glider might potentially breach the anti-bot provisions of ToU that prohibit against bot and unauthorized third-party software, whether using Glider infringes Blizzard's exclusive right remains an issue. The court did not elaborate this issue in detail and held that "Glider does not infringe any of Blizzard's exclusive rights" because "the use [of Glider] does not alter or copy WoW software."[185] As a result, using Glider did not constitute direct copyright infringement and MDY was not liable for secondary infringement.

Because Glider did not constitute copyright infringement, whether certain provisions of Section 1201 prohibit circumvention of access controls when access does not constitute copyright infringement is a new issue. The court analyzed these issues on whether MDY is liable under the DMCA Section 1201(a)(2) and Section 1201(b)(1), which will be discussed below.

iii. Circumvention of copyright protection system

There are three issues regarding unauthorized circumvention in *Blizzard*: (1) whether Warden constitutes a TPM; (2) whether Glider violates Section 1201 by circumventing Warden; and (3) whether the action of circumventing Warden infringes Blizzard's copyright. Warden was an anti-cheating software that scans the computer's RAM before and during the game. It halts the computer's copying of copyright code from the hard drive to the RAM if it detects unauthorized third-party software. After Warden was launched, MDY programmed Glider to avoid detection by Warden. Blizzard considered Warden as a TPM that control access to WoW and therefore, protect the copyright of Blizzard. It alleged that MDY violated the DMCA Section 1201(a)(2) and Section 1201(b)(1).

---

[184] *Id*. at 940.
[185] *Id*. at 941.

In *Blizzard I*, the district court categorized WoW into three copyright components: (1) literal elements such as source code stored on hard drives; (2) individual non-literal elements such as visual images or its audible files stored on hard drives; and (3) dynamic non-literal elements that is "the real-time experience of traveling through different worlds, hearing their sounds, viewing their structures, encountering their inhabitants and monsters, and encountering other players,"[186] which requires connection to a Blizzard server. With respect to the literal code and non-literal files, the court concluded that Warden did not prevent WoW players from gaining access to these elements because they could be accessed on the hard drive without connecting to a game server and encountering Warden. Therefore, Warden was not a TPM covered by Section 1201(a)(2).

With respect to the dynamic non-literal elements, the court adopted a six-part test in *Chamberlain Group, Inc. v. Skylink Technologies, Inc.*[187] The most important prong in this six-part test[188] is the "infringement nexus requirement" that requires plaintiff, who alleges violation of Section 1201(a), to demonstrate that the circumventing technology infringes or facilitates infringement of plaintiff's copyright. In other words, to claim that MDY violates Section 1201(a), Blizzard needs to prove that Glider constitutes copyright infringement.

Because the district court held MDY was liable for secondary copyright infringement, it ruled for Blizzard because the real-time experience of playing WoW could not be accessed without connecting to a Blizzard server, and Warden effectively controlled access to these elements. Accordingly, Warden constituted a TPM and MDY violated Section 1201(a)(2) and 1201(b)(1).

---

[186] *Blizzard I*, at 966.

[187] *Chamberlain Group, Inc. v. Skylink Technologies, Inc.*, 381 F.3d 1178 (Fed Cir. 2004)

[188] *Chamberlain*, at 1203: "A plaintiff alleging a violation of Section 1201(a)(2) must prove: (1) ownership of a valid copyright on a work, (2) effectively controlled by a technological measure, which has been circumvented, (3) that third parties can now access (4) without authorization, in a manner that (5) infringes or facilitates infringing a right protected by the Copyright Act, because of a product that (6) the defendant either (i) designed or produced primarily for circumvention; (ii) made available despite only limited commercial significance other than circumvention; or (iii) marketed for use in circumvention of the controlling technological measure."

Notably, in *Chamberlain*, the Federal Circuit concluded that Section 1201(a) created a new cause of action linked to copyright infringement,[189] therefore plaintiff who alleged Section 1201(a)(2) was required to demonstrate a nexus to infringement. However, the infringement nexus requirement was rejected by the Ninth Circuit in *Blizzard II*, which will be analyzed below.

In *Blizzard II*, because the court of appeals reversed the district court's decision by holding that Glider did not constitute copyright infringement, the court first considered whether circumventing technology constitutes copyright infringement is a prerequisite for copyright owners alleging violation under Section 1201(a)(2). By construing the plain language of the statute and relevant legislative history,[190] the court concluded that "section (a) creates a new anticircumvention right distinct from copyright infringement, while section (b) strengthens the traditional prohibition against copyright infringement."[191] Therefore, Section 1201(a)(2) prohibits trafficking in technology that facilitates circumvention of access-control TPM, regardless of whether such technology constitutes copyright infringement or not. Section 1201(b)(1) prohibits trafficking in technology that facilitates circumvention of TPMs that protect a copyright owner's right against infringement. Applying this rationale, the court of appeals agreed with the district court's decision with respect to the literal and individual non-literal elements of WoW, but adopted a different approach with respect to WoW's dynamic non-literal elements.

On determining whether MDY violated Section 1201(a)(2) with respect to WoW's dynamic non-literal elements, the court of appeals did not follow the six-part test from *Chamberlain*, but adopted its own "six textual elements" test based on the construction of the

[189] *Chamberlain*, 381 F.3d, at 1192-1193.
[190] *See* H.R.Rep. No. 105–551 pt. 2, at 23 (1998): "content providers will need both the technology to make new uses possible and the legal framework to ensure they can protect their work from piracy."
[191] *Blizzard II*, at 948.

statute.[192] Accordingly, the court agreed with the district court's holding that WoW's dynamic non-literal elements constitutes an independent copyrighted work because a player can either screenshot or record the audiovisual game displayed. Notably, the court also recognized Warden as an effective access control measure of WoW based on Section 1201(a)(3)(B)[193] because Blizzard launched Warden to scan a computer's RAM and control player's access to a game server, which controlled a player's access to WoW's dynamic non-literal elements. As a result, the court held that MDY was liable under Section 1201(a)(2).[194]

On determining whether MDY violated Section 1201(b)(1) with respect to WoW's dynamic non-literal elements, the court of appeals concluded that Warden did not protect WoW's reproduction right against unauthorized copying because it was designed to reduce the presence of cheats and bots. Although Glider avoided or bypassed the detection by Warden, it did not infringe or facilitate Glider users to infringement. Therefore, MDY was not liable under Section 1201(b)(1).[195]

As a result, MDY is only liable under Section 1201(a)(2) because Warden controlled access to WoW. However, the court indicated that if a copyright owner puts in place an effective measure that both controls access and protects against copyright infringement, a defendant who traffics in a technology that circumvents that measure could be liable under both Section 1201(a) and (b).[196] If game companies such as Blizzard seek more protection under Section 1201, adopting TPMs that controls access and protects against copyright infringement could be an effective way to fight against unauthorized third-party programs.

---

[192] *Blizzard II*, at 954.
[193] 17 U.S.C. § 1201(a)(3)(B): "a technological measure 'effectively controls access to a work' if the measure, in the ordinary course of its operation, requires the application of information, or a process or a treatment, with the authority of the copyright owner, to gain access to the work"
[194] *Blizzard II*, at 954.
[195] *Blizzard II*, at 955.
[196] *Blizzard II*, at 946.

iv. A new challenge for game industry against unauthorized third-party program

With the development of live streaming and Video on Demand (VOD) businesses, the game industry is facing a new challenge on unauthorized third-party program such as bot, cheat, hack or plugin. To attract subscribers and earn more money from online video platforms, some gamers who provide game content on their live streaming or VOD channels use unauthorized third-party program. For example, a gamer who played, modified or hacked versions of Fortnite[197] and other games attracted 1.7 million subscribers to his YouTube channel.[198] Moreover, this gamer even ran a website that promoted, advertised and sold cheating software. Thus, the gamer has created a financial loop from both sides. When his YouTube channel became more popular by using cheat software, his website sold more cheat software to his subscribers. When the old cheat software was blocked by the game company, the gamer earned enough money for cheat software developer to program a new one.

Although almost all the game companies strictly prohibit cheating and force players agree to that in ToU or EULA, they are reluctant to block all the third-party programs for their games because some third-party programs are not cheat. For example, BigFoot is an authorized third-party plugin for WoW. When the WoW players fight against a boss in the game, BigFoot warns the players 5 seconds before the boss releases a bomb, and marks the bomb area on the map so that the players can avoid the damage. However, most of the third-party programs for video game are unauthorized by the game company and potentially infringe the copyright of the game.

For example, Fortnite Battle Royale allows less than one hundred players land on a map, look for weapons and equipment, and build defenses. The players fight each other until only

[197] Fortnite is a popular online video game developed by Epic Games and first released in 2017. It has more than 75 million players around the world and is the most viewed game on streaming site Twitch.
[198] BBC, *Fortnite cheat YouTuber sued by Epic Games*, Oct. 16, 2018. Available at https://www.bbc.com/news/technology-45876864.

one player stands. One of the hacks for Fortnite Battle Royale is aimbot, which allows players to automatically target and kill enemies without having to aim their weapons manually. By using aimbot, a player gains an unfair advantage against players who are playing fairly. In October 2018, Epic Games took over an anti-cheat software firm Kamu to tackle unauthorized programs to its games.[199] According to *Blizzard II*, the provider of aimbot is likely to violate Section 1201(a)(2) for circumventing anti-cheat software, but is not necessarily liable for copyright infringement.

Another way to gain an unfair advantage in Fortnite Battle Royale is to change the default skin of the character. By using a skin hack, a player can modify the appearance of the character to a similar color of the background or even invisible so that other players find it hard to aim at a modified character. Under Copyright Act, not only does a skin hack potentially violate Section 1201 for circumventing anti-cheat software, but also infringes Epic Games' copyright on Fortnite's character, such as literal code and non-literal audiovisual files. By unlawfully modifying the game's literal code of a character, a skin hack creates unauthorized derivative works of Fortnite's character.[200] Therefore, a skin hack potentially infringes Epic Games' reproduction right of Fortnite's literal code and derivative right of Fortnite's non-literal audiovisual elements.[201]

An effective way for game companies to tackle unauthorized third-party programs is adopting anti-cheat software, such as Blizzard adopting Warden in WoW. According to *Blizzard II*, the Ninth Circuit indicated that if a copyright owner adopts TPMs that both control access and protect copyright, a defendant who provide a technology that circumvents that TPM could be liable under both Section 1201(a) and (b).[202] Therefore, to gain protection under Section 1201(a), a game company should adopt TPMs that (1) control access to the game; and (2) detect

---

[199] *Id.*
[200] *Id.*
[201] *Id.*
[202] *Blizzard II*, at 946.

and block unauthorized third-party programs. To gain protection under Section 1201(b), a game company should adopt TPMs that prevent unauthorized modification to its copyright, including literal, non-literal and dynamic non-literal elements of the game.

Another effective way for game companies to tackle unauthorized third-party programs is cooperating with online intermediaries, such as YouTube or Twitch. For example, Epic Games filed a copyright complaint to YouTube in order to remove videos that involves aimbot cheat.[203] Blocking gamers who use cheat from online video platform damages the financial loop of the cheat, because these cheaters are likely to lose subscribers and income from the video channel. Eventually, when the cheaters do not have enough income to pay the cheat software developer, the financial loop of the cheat ends.

Nonetheless, it is possible that the online video platforms are reluctant to block their popular channels. As mentioned before, an ISP is not liable for secondary copyright infringement under safe harbor doctrine. This issue will be addressed in the *YouTube* case below.

d. Viacom v. Google/YouTube

One of the most recent cases about ISP's safe harbor doctrine is *Viacom v. Google/YouTube* (hereinafter "*YouTube II*").[204] 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 User Generated Content (UGC) websites that allows its users to watch, upload, and share personal clips on its website and watch the video free of charge.[205] 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 that requires the user "not [to] 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

[203] BBC, *Fortnite cheat YouTuber sued by Epic Games*, *supra* note 198.
[204] *Viacom Int'l, Inc. v. YouTube, Inc.*, 676 F.3d 19 (2d Cir. 2012).
[205] *Id.* at 28.

rights granted herein."[206] After the registration is completed, the user is able to upload any videos from 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 for other users on the Internet.

i. Actual knowledge provision

In the *YouTube I case*,[207] the district court applied the actual knowledge provision Section 512(c)(1)(A)(i)[208] and "Red Flag" knowledge provision Section 512(c)(1)(A)(ii)[209] to determine whether an ISP qualifies for the Section 512(c) safe harbor protection. The district court believed that the critical question was 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." The court of appeals 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."[210] Furthermore, the court of appeals pointed out a subjective and objective standard between the 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.[211]

In other words, the subjective standard refers to actual knowledge of specific infringement,

---

[206] *Id.*
[207] *Viacom Int'l, Inc. v. YouTube, Inc.*, 718 F. Supp. 2d 514, 519 (S.D.N.Y. 2010).
[208] 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;
[209] 17 U.S.C. § 512(c)(1)(A)(ii): in the absence of such actual knowledge, is not aware of facts or circumstances from which infringing activity is apparent;
[210] *Id.* at 523.
[211] *Viacom,* 676 F.3d at 31.

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.[212]

ii. Red flag provision

Generally, an ISP may know that its service may be used for 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 the 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. First, the ISP must be unaware of facts that indicate specific and identifiable instances of infringement. Second, the ISP must ensure an expeditious removal after it knows exactly which items to remove.

Even if an ISP qualifies for safe harbor protection under Section 512(c)(1)(A), Section 512(c)(1)(B) requires an ISP to "ha[ve] the right and ability to control" the infringing activity. In *YouTube I*, the district court believed that "an ISP must have specific knowledge of the infringing activity before he can control."[213] While the Court of Appeals held that "§512(c)(1)(B) does not include a specific knowledge requirement" and "requires something

[212] *UMG Recordings, Inc. v. Shelter Capital Partners LLC*, 718 F.3d 1006, 1026 (9th Cir. 2013).
[213] *Viacom,* 718 F. Supp. 2d at 527.

more than the ability to remove or block access to materials posted on a service provider's website."[214] Nonetheless, the Court did not discuss this so-called "something more" standard in depth. Consequently, the question becomes how an ISP should act in order to qualify for safe harbor protection under Section 512(c)(1)(B).

iii. Something more standard

The Court provided two examples to demonstrate the something more standard, an ISP "exert substantial influence on the activities of users" such as "institute a monitoring program" or "forbid certain types of content and refuse assess to users who failed to comply with its instructions."[215] 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."[216] In *YouTube II*, the 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."[217]

As a conclusion from *YouTube I & II*, the something more standard requires an ISP to show its 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. Moreover, the something more standard indicates that the court actually requires ISPs to take active steps to prevent copyright infringement instead of hiding behind the safe harbor protection.

4. Conclusion

As one of the most developed country in the world, the U.S. has accumulated a lot of

---

[214] *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).
[215] *Id. See also Perfect 10, Inc. v. Cybernet Ventures, Inc.*, 213 F.Supp.2d 1146 (C.D.Cal.2002).
[216] *UMG Recordings, Inc. v. Shelter Capital Partners LLC*, 718 F.3d 1006, 1030 (9th Cir. 2013).
[217] *Viacom,* 718 F. Supp. 2d at 528.

legal experience on the copyright infringement issues of ISPs. On the other hand, China is also facing the similar issues of ISPs. The Chinese legislature has adopted multiple legal theories from the U.S. as a reference to solve the issues of ISPs in China before the E-commerce Law. Part B of this chapter introduces the Chinese approach to the secondary copyright infringement liability of ISPs.

B. Secondary copyright Liability of ISPs in China

Part B of this chapter discusses the development of secondary copyright liability of ISPs in China, with a comparative analysis of the U.S. law in Part A. Section 1 introduces background information about Chinese policy of ISPs before the E-commerce law. Section 2 analyzes the impact of the E-commerce law for ISPs and discusses the active-preventive approach of ISPs in China.

1. China's approach to the copyright liability of ISPs before E-commerce Law

This section first introduces the differences between Chinese legal system and American legal system, then presents the laws and regulations of ISPs in China before the new promulgated E-commerce law with a comparative analysis of the U.S. law.

a. Background

Unlike the U.S. common law system, China is a civil law country. According to the Legislation Law of the PRC,[218] the legal effect of the Constitution is the highest.[219] Law is higher than administrative regulation.[220] When applying a new legal principle, the Chinese

[218] Zhong hua ren min gong he guo li fa fa (中华人民共和国立法法) [Legislation Law of the PRC] (promulgated by the Nat'l People's Cong., Mar. 15, 2015, effective in Mar. 15, 2015). The English translation is available at http://app.westlawchina.com/maf/china/app/document?&docguid=i3cf76ad10000014c20983ba61082ea37&hitguid=i3cf76ad10000014c20983ba61082ea37&srguid=i0ad82a4100000166c5f1767c22b4babf&spos=2&epos=2&td=3&crumb-action=append&context=30&lang=en.

[219] Legislation Law of the PRC, art. 87.

[220] Legislation Law of the PRC, art. 88 para.1.

legislation tends to enact it in a regulation for trial implementation. If the new principle works well during the trial implementation period, the Chinese legislation will consider enacting it into a law. Notably, the case law is not legally binding in China, and the Chinese legislation merely consider case law as a reference.

Pushed by WTO and the U.S., the Chinese legislation began to enact principles of ISPs after 2000. As mentioned before, the DMCA was enacted in 1998 and the copyright liability theory of ISPs were well-developed in the U.S. Therefore, the Chinese legislature was influenced by the model of ISPs in the U.S. This section introduces the legislation history of copyright liability of ISPs in a chronological order.

b. Statutory development of the copyright liability of ISPs in China

i. Copyright Law of the PRC

As mentioned before in Chapter II, Copyright Law of the RPC was revised twice upon the international pressure from the U.S. and WTO, therefore, most the amendments follow the standards from the TRIPs and the DMCA.[221] The 2001 Copyright Law was amended to fulfill the requirements of TRIPs. The 2010 Copyright Law provides limited protection to copyright owners in the digital world because it only defines some broad concepts and basic rights of copyright. With the rapid development of network technology and business, the legal uncertainties of the 2010 Copyright Law became serious. For example, live streaming became popular after 2010, and the scale of live webcast users reached 422 million in 2017.[222] However, whether live streaming shall be regulated under the right of broadcasting[223] or the

[221] Zuo Yuru (左玉茹), Comments on the Draft of the Third Amendment of the Copyright Law (《著作权法》第三次修改草案述评), Electronics Intellectual Property (电子知识产权), No. 4, 2012 at 24.
[222] CNNIC, 41st Statistical Report on Internet Development in China, *supra* note 11, at 8.
[223] 2010 Copyright Law, art. 10 para. 11: "Right of broadcasting, i.e., the right to publicly broadcast or disseminate a work through wireless transmission, to disseminate a broadcast work to the public through wire transmission or rebroadcast, and to disseminate a broadcast work to the public through a loudspeaker or any other similar instrument used to transmit symbols, sounds, or images."

right of dissemination via information network is disputed because both rights cover live streaming.[224] The Chinese legislature has already noticed the problems and a third revision of Copyright Law is in progress. The Draft of the Third Amendment of the Copyright law will be discussed later in Section 2.

The 2010 PRC Copyright Law did not provide much detail on ISPs because the Chinese legislation enacted provisions of ISPs into regulations for trial implementation. These regulations will be discussed below.

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

After the 2001 Copyright Law, the 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. The ICM first adopted the Safe Harbor model from the U.S. DMCA, such as the N&T provision for trial implementation. For example, Article 5 of the 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." [225] However the ICM became obsolete because the RPRD was promulgated one year later.

iii. RPRD

The specific regulations about ISP can be found in the RPRD, which was promulgated in 2006 and revised in 2013. The Chinese legislature has followed the safe harbor model in the U.S. to regulate ISP liability and limitation. As mentioned before in Chapter II, the RPRD

[224] Zuo, *supra* note 221, at 20.

[225] 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 the NCA & MII, Apr. 29, 2005, effective May 1, 2005), art 5, translated by Bei da fa bao (北大法宝) (en.pkulaw.cn) [hereinafter ICM].

stipulates four categories of ISP conducts under liability exemptions subject to certain conditions, which is similar to Section 512 of the DMCA. Although the expression of the RPRD Article 20-23 is not exactly the same as the DMCA Section 512(a)-(d), the four categories of ISP conducts between the two countries have almost the same function. For example, Article 21 exempt ISPs that provide "automatic storage service"[226] from the liability for compensation while the term in Section 512(a) is "system caching."

Notably, Article 22 of the RPRD adopts the secondary copyright liability theory of ISPs and provides similar provisions in Section 512(c).[227] For example, Item (3) of Article 22 stipulates that ISPs are not liable if they do not know or have justifiable reasons to know about the infringing activities of the subscribers. The actual knowledge provision and the Red Flag provision in Section 512(c)(1)(A) also require that the ISPs do not have "actual knowledge" about the infringement. Item (4) of Article 22 adopts vicarious liability theory and stipulates that ISPs are not liable if they do not obtain any economic benefits from the infringing activity. Section 512(c)(1)(B) also requires that the ISPs do not "receive a financial benefit." Item (5) of Article 22 stipulates that ISPs shall remove the works in question upon receiving notice from the copyright owners. Section 512(c)(1)(B) also require that the ISPs shall respond expeditiously to remove the infringing materials. As a result, the Chinese safe harbor model

[226] RPRD *supra* note 45, art. 20.

[227] RPRD, art. 22: A network service provider shall be exempted from liability for compensation when providing those who receive its services with information storage space so as to enable them to make works, performances, or sounds or visual recordings available to the public via information network, provided that the following conditions are met:
(1) The information storage space is clearly indicated as having been provided for use by those who receive its services, accompanied by an announcement on the name, contact person, and Web address of the Web service provider;
(2) It has not altered the works, performances, or sound or visual recordings provided by those who receive its services;
(3) It is unaware of, and has no justified reason to be aware of, the infringement of a work, performance, or sound or visual recording provided by anyone who receives its services;
(4) It has gained no economic benefits directly from works, performances, or sound or visual recordings provided by those who receive its services; and
(5) It has, pursuant to these Regulations, deleted the work, performance, or sound or visual recording regarded by the right owner as involving infringement after receiving the right owner's written notice.

also adopts the red flag test[228] and the secondary copyright liability theory established in American case law.[229]

Moreover, the RPRD also adopted the anticircumvention provision that is similar to Section 1201 of the DMCA. For example, Article 4 of the RPRD provides that: "For the purpose of protecting the right of dissemination via information network, the owner can take a technological measure." Although the second paragraph of Article 4[230] also prohibits circumventing TPMs and trafficking in technology that facilitates circumvention of TPMs, the definition of the term "technological measure" in RPRD is different from the term "technological measure" in Section 1201(a). According to Article 26, technological measure" in RPRD refers to any effective technology used to prevent or restrict (1) the browsing or enjoyment of a work, or (2) the making available to the public via information network of a work.[231] Section 1201(a) refers to "a technological measure that effectively controls access to a work." The definition difference of the term "technological measure" between Article 26 of the RPRD and Section 1201(a) of the DMCA will be discussed through a case in Section C below.

iv. Tort Liability Law of the PRC

After enacting the model U.S. of ISPs into regulations for trial implementation, the Chinese legislation enacted the liability of ISPs into the Tort Liability Law in 2010. Different

---

[228] 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.

[229] HUA, *supra* note 105, at 111.

[230] RPRD, *supra* note 45, art. 4 para. 2: "No organization or person shall intentionally avoid or destroy the technological measures, shall intentionally manufacture, import, or provide the public with devices or components mainly used to avoid or destroy the technological measures, and shall intentionally provide technical services to others to avoid or destroy the technological measures, unless it is provided for by any law or administrative regulation that the technological measures may be avoided."

[231] RPRD, *supra* note 45, art. 26 para. 2: "Technological measure shall mean any effective technology, device or component used to prevent or restrict the browsing or enjoyment of a work, performance, or sound or visual recording that is not authorized by the right owner or the making available to the public via an information network of a work, performance, or sound or visual recording."

from the direct and secondary copyright infringement theories of ISPs in the U.S., China adopted the "Joint-Liability" theory of ISPs that originates in Tort Liability Law and stems from the joint liability principle in the General Rules on the Civil Law of the PRC (Civil Code of the PRC).[232] The Civil Code of the PRC was first enacted in 1986, and the new Civil Code of the PRC was promulgated and came into effect in 2017. Article 178 of the Civil Code provides that: "If two or more persons bear joint and several liability according to law, the right holder shall be entitled to pursue obligations against some or all parties who are jointly and severally liable."[233] The Tort Liability Law was promulgated in 2010 and applied the joint-liability theory on the liability of ISPs. The principle of Joint-Liability can be found in the Tort Liability Law Article 9: "One who abets or assists another person in committing a tort shall be liable jointly and severally with the tortfeasor."[234] And the specific provision of ISPs was enacted in Article 36, which can be divided into two parts: direct infringement and secondary infringement.

The first paragraph of Article 36 stipulates that both ISPs and network users are liable if they directly infringe another person's civil rights.[235] Notably, the civil rights in the Civil Code of the PRC include IP rights,[236] therefore, the scope of Article 36 is broader than Section 512 of the DMCA.

The second paragraph of Article 36[237] is similar to Section 512(c)(1)(C), which

---

[232] Zhong hua ren min gong he guo min fa zong ze (中华人民共和国民法总则) [General Rules on the Civil Law of the People's Republic of China] (promulgated by the Nat'l People's Cong., Mar. 15, 2017, effective in Oct. 1, 2017). The English translation is available at http://app.westlawchina.com/maf/china/app/document?&docguid=i000000000000015ad4d7e58b663a38f6&hitguid=i000000000000015ad4d7e58b663a38f6&srguid=i0ad6283300000166b6e31d3952fec806&spos=1&epos=1&td=476&crumb-action=append&context=3&lang=en

[233] Civ. Code of the PRC, art. 178.

[234] Tort Liability Law, *supra* note 51.

[235] Tort Liability 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."

[236] Civ. Code of the PRC, art. 123: "A civil subject shall be entitled to intellectual property rights in accordance with the law."

[237] Tort Liability Law, art. 36 para. 2: "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

stipulates that ISPs are secondary liable for their users' direct infringement if they fail to finish the N&T requirement. Moreover, the third paragraph of Article 36 is similar to Section 512(c)(1)(A) and provides that "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."[238] Although China applies the joint-liability theory on ISPs instead of the contributory or vicarious theories applied in the U.S., the people's courts in China considered similar factors on secondary infringement liability of ISPs based on the expression of the Article 36. However, merely one article in the Tort Liability Law is not enough to solve complicated issues of ISPs. Therefore, in determining the issues of ISPs, the People's Courts highly relied on the "judicial interpretation," which will be discussed below.

v. Judicial interpretation of the Right of Dissemination via Information Networks

One legal issue regarding to the ISPs in China is that Article 36 of Tort Law merely stipulates general principles of ISPs, therefore, does not provide much detail for people's courts on how to solve practical issues of ISPs. Nonetheless, according to the Organic Law of the People's Courts of the PRC,[239] the Supreme People's Court can provide a judicial interpretation on a specific legal issue.[240] Generally, all the Chinese lower courts are supposed to comply with the Supreme People's Court's judicial interpretation. Compared to the U.S. legal system, the effect of judicial interpretation of the Supreme People's Court is similar to the effect of the U.S. Supreme Court's opinion. Therefore, the Opinion and Interpretation published by the Supreme People's Court are very important legal materials in China.

---

user."

[238] Tort Liability Law, *supra* note 51, art. 36.

[239] Zhōnghuá rénmín gònghéguó rénmín 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 PRC] (promulgated by the St. Council, Jul 1, 1979, amended by the St. Council in Oct 26, 2018, effective in Jan 1, 2019) (China). Translated by Westlawchina (www.westlawchina.cn).

[240] Organic Law of the People's Courts of the PRC, art. 18, para. 1: "The Supreme People's Court gives interpretation on questions concerning specific application of laws and decrees in judicial proceeding."

With regard to the issues of ISPs, the Supreme People's Court of the PRC published the "Provisions of the Supreme People's Court on Certain Issues Related to the Application of Law in the Trial of Civil Cases Involving Disputes over Infringement of the Right of Dissemination via Information Networks" (2012 Provision).[241] The 2012 Provision interprets some statutes from the RPRD in detail and guides the lower People's Court on how to apply the laws to specific cases. For example, Article 36 of the Tort Law does not mention whether copyright owners or ISPs shall bear the burden of proof on the direct infringement liability. Article 4 of the 2012 Provision solved this issue by providing that "if the network service provider is able to provide evidence . . . the people's court shall support such a claim of the network service provider."[242] Therefore, the ISP should bear the burden of proof based on Article 4 of the 2012 Provision.

Another issue involving the ISPs' secondary infringement liability in Article 36 of the Tort Law is how to determine whether the ISPs have "actual knowledge" about the infringement activities. To solve this issue, the 2012 Provision adopted some principles from American case law such as the Red Flag provision.[243] Article 9 of the 2012 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

---

[241] 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 via Information Networks] [hereinafter "the 2012 Provision"](promulgated by the Sup. People's Ct., Dec. 12, 2012, effective Jan. 1, 2013) Interpretation No. 20 (2012) [法释(2012)20 号] of the Sup. People's Ct. translated by Bei da fa bao (北大法宝) (en.pkulaw.cn) [hereinafter 2012 Provision].

[242] 2012 Provision, *supra* note 241, 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."

[243] Lin Chengduo(林承铎) & An Nita(安妮塔) Application of Digital Copyright Laws in the Context of Safe Harbor Agreement and Red Flag Test (数字版权语境下避风港规则与红旗原则的适用), Electronics Intellectual Property (电子知识产权), No. 7, 2016, at 22.

> the works, performance, and audiovisual 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."[244]

As mentioned before in the *YouTube* case, the Second Circuit also examined how to determine whether the ISPs have "actual knowledge" about the infringement activities and applied subjective and objective standards. As a result, the 2012 Provision adopted a similar test from American case law.

In addition, not only did the 2012 Provision adopt rationales from American case law, but also developed and modified the U.S. legal theories of ISPs based on China's national conditions. For example, in *YouTube*, the Second Circuit discussed "something more" standard that require ISPs to actively prevent their users from infringing activities. The 2012 Provision also adopted this rationale in Article 11 Paragraph 1:

> Where a network service provider has directly obtained economic benefits from any works, performance or audio-video product made available by a web user, the people's court shall decide that it has a higher duty of care towards such web user's act of infringement of the right of dissemination through information networks.[245]

Moreover, because the online piracy issues in China are more serious than in the U.S., the 2012 Provision developed the "something more" standard from *YouTube*, and imposed "a higher duty of care" on ISPs that "directly obtained economic benefits from" the UGC. The purpose of Article 11 is to force some categories of ISPs to actively prevent their users from copyright infringement. Nonetheless, neither the 2012 Provision nor the Tort Liability Law explain the term "duty of care," which creates huge legal uncertainties on the duty of care requirement of ISPs. Because the criteria of duty of care is unclear, the people's courts construe duty of care requirement in different extents when applying this requirement on ISPs. The duty of care

[244] 2012 Provision, *supra* note 241, art. 9.
[245] 2012 Provision, art. 11 para. 1.

requirement of ISPs will be further analyzed in *Baidu* and *SOHO* cases in Section C.

vi. Judicial interpretation of the duty of care

Although the Supreme People's Court does not provide further explanation on the higher duty of care of ISPs in the 2012 Provision, in the "Interpretation of the Supreme People's Court on Certain Issues Concerning the Application of Law in the Trial of Civil Cases Involving Copyright Disputes" (2002 Interpretation),[246] Article 20 of the 2002 Interpretation imposes an "obligation of due care" on the publisher, which could be considered as a reference to the duty of care requirement. Article 20 of the 2002 Interpretation provides that:

> Where a publisher fails to perform the obligation of due care for matters such as the authorization granted to the publisher's act of publishing, the source or authorship of a work contributed to a publication edited by the publisher, or the content of such a publication, the publisher shall bear compensation liability in accordance with the provisions of Article 48 of the Copyright Law.
> Where a publisher has performed the obligation of due care and the copyright owner does not have any proof showing that the publisher should have known that the publishing thereof involved infringement, the publisher shall bear civil liability, in accordance with the provisions of Paragraph 1 of Article 117 of the General Principles of the Civil Law, to stop the infringement and refund the amount of profit resulting from the infringement.
> The publisher shall bear the burden of proof to show that it carried out the obligation of due care.[247]

Article 20 stipulates that a publisher is strictly liable for copyright infringement in its publication. In other words, obligation of due care requires the publisher to actively verify the copyright information of its publication, otherwise the publisher shall bear compensation liability if its publication infringes on copyright. If the publisher performs the obligation of due care but its publication still infringes on copyright, it shall not bear compensation liability, but

[246] Zui gao ren min fa yuan guan yu sheng li zhu zuo 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著作权民事纠纷案件适用法律若干问题的解释) [Interpretation of the Supreme People's Court on Certain Issues Concerning the Application of Law in the Trial of Civil Cases Involving Copyright Disputes] (promulgated by the Sup. People's Ct., Oct. 12, 2002, effective Oct. 15, 2002) Interpretation No. 31 [2002] of the Sup. People's Ct. (China). Translated by Westlawchina (www.westlawchina.cn) [hereinafter 2002 Interpretation].

[247] 2002 Interpretation, art. 20 para. 2-4.

it is responsible to stop the infringement and refund the profit to the copyright owner.[248]

Analogized to ISPs, publishers are responsible for their publications because they have to edit the content before distribution. On the contrary, the ISPs do not have affirmative duty to screen, select, or edit the uploaded content from their users. Paragraph 2 Article 8 of the 2012 Provision follows Section 512(m) of the DMCA and stipulates that it is unnecessary for ISPs to "take initiative to examine a web user's act of infringement."[249] However, for certain ISPs that directly obtained economic benefits from the UGC, they have a higher duty of care to affirmatively examine whether the UGC from web users involves copyright infringement. As a result, the higher duty of care adopts the rationale from the obligation of due care of publishers in certain circumstance. It requires ISPs to actively verify the copyright information of the UGC from web users when they have justifiable reason to know the existence of the infringement.

vii. Summary

In sum, the 2012 Provision adopted some rationales of ISPs from American case law and developed some unique approaches on the issues of ISPs based on the national conditions of China, such as duty of care requirement. Before the E-commerce Law, courts refer to joint-liability theory when deciding the cases about secondary copyright infringement, and particularly assess whether an ISP fulfills its duty of care to prevent infringement.[250] Because the duty of care requirement is unclear in the 2012 Provision, Part II Section C analyzes two cases of ISPs to further explain how people's courts applies duty of care requirement on ISPs.

---

[248] WANG QIAN (王迁), COPYRIGHT LAW (著作权法) 406 (China Renmin University Press [中国人民大学出版社) 2015).

[249] 2012 Provision art. 8 para. 2: Where a web service provider fails to take the initiative to examine a web user's act of infringement of the right of dissemination through information networks, the people's court shall not decide that it is at fault on these grounds.

[250] JIE WANG, REGULATING HOSTING ISPS' RESPONSIBILITIES FOR COPYRIGHT INFRINGEMENT 10 (Springer 2018).

2. China's new Approach to the Copyright Liability of ISPs

This section first introduces the new promulgated E-commence Law. After analyzing the advantages and drawbacks of this law on the scope of copyright liability, this section discusses the impact of the E-commerce law to the ISPs in China.

a. Background

Based on the huge amount of Internet users, the potential online copyright market in China is tremendous. According to the 41st Statistical Report on Internet Development in China (Jan 2018)[251] from the CNNIC, the number of Chinese Internet users was about 772 million and the penetration rate reached 55.8%, an increase of 2.6 percentage points from the end of 2016.[252] To regulate such a huge online market, the Chinese legislation revised laws and enacted Internet related provisions into regulations in order to provide policy incentives and guidance for its online market. After taking both domestic and foreign systems of ISPs into consideration, the Chinese legislation enacted the E-commerce law to regulate the Chinese online market.

b. The advantages of the E-commerce law

First, one of the significant advantages of the E-commerce law is that it sets up the IPR protection duty of ISPs. Before the E-commerce law, most of the provisions of ISPs were enacted in regulations for trial implementation. Article 41 of the E-commerce law confirms the IPR protection duty of ISPs from different regulations by requesting ISPs to formulate IPR protection rules and cooperate with IPRs holders.[253]

Second, the E-commerce law builds up a complete IP protection mechanism of ISPs. As mentioned before, the RPRD follows the U.S. model of ISPs and regulates ISPs in copyright

[251] CNNIC, 41st Statistical Report on Internet Development in China, *supra* note 11, at 1.
[252] CNNIC, *supra* note 11, at 10.
[253] E-commerce Law, art. 41.

regime for trial implementation. The E-commerce law adopts the legal experiences from the RPRD and enlarges the protection scale from the copyright regime to all IP regimes. For example, Article 45 of the E-commerce law generally adopts the secondary copyright liability theory from U.S. law and enlarges the scale of this theory to all of IP. The first part of Article 45 is similar to Section 512(c) of the U.S. Copyright Act, and requires that if an ISP know or should know that online business operators involve infringement on IPRs, the ISP shall take necessary measures such as deleting, blocking, disconnecting, and terminating transactions or services. Moreover, to suit the national condition of China, the E-commerce law also combine the Joint-Liability theory from the Tort Liability Law. For example, the second part of Article 45 follows Article 36 of the Tort Law and stipulates that the ISP and the infringer shall be jointly and severally liable if the ISP fails to take necessary measures to prevent infringement.[254]

Third, the E-commerce law legally transplants some ISP-related rules from the U.S. Copyright Act. For example, Article 42 paragraph 3 of the E-commerce law is similar to Section 512 (f)[255] that prevent sending false notification to the ISPs. Notably, the compensation is doubled if a violator sends a false notification with malicious intent.[256] Moreover, Article 43 of the E-commerce law also transplants the counter notification provision from Section 512 (g)(3).[257] Paragraph 1 of Article 43 stipulates that if an online business operator receives a notification of infringement, it can submit a statement including prima facie evidence showing that there is no infringement to ISPs.[258]

In conclusion, the advantages of the E-commerce law is that (1) it follows the copyright

[254] E-commerce Law, art. 45.
[255] 17 U.S.C. § 512(f): Any person who knowingly materially misrepresents under this section (1) that material or activity is infringing, or (2) that material or activity was removed or disabled by mistake or misidentification, shall be liable for any damages […].
[256] E-commerce Law, art. 42 para. 3.
[257] 17 U.S.C. § 512(g)(3): To be effective under this subsection, a counter notification must be a written communication provided to the service provider's designated agent […].
[258] E-commerce Law, art. 43 para. 1.

protection model of ISPs in the U.S. and enlarges the protection scale from copyright regime to all IP regimes; (2) it harmonizes the provisions of ISPs that stipulated in different laws and regulations, and set up a unified protection system for all IP regimes; and (3) it legally transplants some ISP-related rules from the U.S. Copyright Act and modifies the rules to suit the national condition of China.

c. Drawbacks of the E-commerce law in copyright regime

Following the U.S. model of ISPs from the Copyright Act and enlarging the protection scale to all IP regimes can be a double-edged sword for the E-commerce law. A complete IPRs protection mechanism of ISPs is necessary for China, but an IPRs protection mechanism that stems from a copyright protection mechanism also creates huge legal uncertainties on the IPRs protection of ISPs.

First, whether the model of ISPs for copyright protection can effectively protect all IP regimes is questionable. As mentioned in Section A, the Chinese legislation tends to stipulate new legal principles into regulations for trial implementation before enacting them into a law. Since the RPRD regulated copyright model of ISPs that originates from the U.S. Copyright Act for years, enacting copyright model of ISPs from the RPRD to the E-commerce law is reasonable. However, not only does the E-commerce law transplant the model of ISPs from the U.S. Copyright Act, but also enlarges the protection scale to other IP regimes without trial implementation. Therefore, it is uncertain to determine whether the copyright model of ISPs can effectively work on the other IP regimes, such as trademark. Because this Chapter focuses on copyright, the trademark issues of the E-commerce law will be discussed later in Chapter IV.

Second, the E-commerce law is not applicable to several Internet content providers, which is debatable because such exclusion contradicts the IP protection mechanism of ISPs. The E-commerce law follows the model of ISPs from the U.S. Copyright Act and enlarges the

protection scale to all IP regimes, but paragraph 3 of Article 2 stipulates that "this law is not applicable to … the use of information networks to provide content services such as news information, audio-visual programs, publications and cultural products."[259] In other words, the E-commerce law sets up an IP protection mechanism for ISPs, but it lists several Internet content providers as exceptions to the definition of E-commerce. Thus, the E-commerce law sets up a model of ISPs that covers all IP regimes, but it also excludes ISPs that provide copyright content services. Ironically, the model of ISPs in the E-commerce law even originates from a copyright model of ISPs.

The technology giant Amazon is a good example to explain the drawbacks of excluding Internet content providers in the E-commerce law. Amazon, Inc. constitutes an e-commerce platform operator under Article 9 of the E-commerce law. Besides providing online shopping services as Amazon.com, Amazon, Inc. also provides content services such as Amazon Music, Amazon Video and Kindle E-books. Because Article 2 excludes Internet content providers such as "audio-visual programs and publications," Amazon Music, Amazon Video and Kindle E-books constitute exceptions under Article 2. With regards to the copyright liability of Amazon, Inc., the E-commerce law sets up copyright liability for Amazon.com, but excludes Amazon Music, Amazon Video and Kindle E-books even though these Internet content service contain massive amounts of copyrighted works. As a result, although Article 41 clearly requires ISPs to formulate IPR protection rules and cooperate with IPRs holders,[260] only Amazon.com is subject to protect copyright under the E-commerce law.

According to the Chinese legislative history, the main reason why the Chinese legislation excludes Internet content providers from the E-commerce law is to avoid legal conflict with the current provisions of ISPs and the ongoing third amendment of the Copyright

[259] E-commerce Law, art. 2 para. 3.
[260] E-commerce Law, art. 41.

Law.[261] The legislative history indicates that the third amendment of the Copyright Law intends to amend the right of broadcasting to right of display[262] and redefine the right of dissemination via information network.[263] Under these circumstances, because the RPRD that regulates the copyright liability of ISPs stipulates the principles of ISPs, it is highly possibly that the RPRD will be abolished after the trial implementation as a regulation. The new amendment of Copyright Law will adopt the principles of ISPs from the RPRD and provide a comprehensive system to regulate copyright liability of ISPs. Therefore, it is possible that the E-commerce law does not stipulate provisions that relate to Internet content providers because (1) the current RPRD regulates the Internet content providers; and (2) the Chinese legislation plans to abolish the RPRD after its trial implementation and enact relevant provisions into the new amendment of Copyright Law.

However, whether the Chinese legislation should exclude Internet content providers from the E-commerce law is still arguable. On one hand, enacting provisions that relate to Internet content providers into the third amendment of the Copyright law is acceptable because (1) potential legal conflict among different laws and regulations can be avoided; (2) the ISPs that specialized in providing copyrighted content service can be regulated under copyright law in the future; and (3) amending the right of broadcasting and the right of dissemination via information network significantly affects the ISPs that provide online streaming services. On the other hand, if E-commerce law does not exclude Internet content providers, (1) there would be no contradiction between Article 2 and Article 41; (2) the E-commerce law would provide a comprehensive IP protection system of ISPs; and (3) the legal uncertainties between the E-commerce law and current provisions of ISPs would be reduced.

In conclusion, the drawbacks of E-commerce law are: (1) it sets up an IP protection

[261] *See* NPC Law Committee, *supra* note 89. *See also* NPC Constitution and Law Committee, *supra* note 90.
[262] 2014 Copyright Draft, *supra* note 30, art. 13, para. 2, subpara. 6.
[263] Zuo *supra* note 221, at 19.

mechanism of ISPs originated from the U.S. Copyright Act without trial implementation; and (2) paragraph 3 of Article 2 contradicts the principle of Article 41 by excluding some Internet content providers from E-commerce law. These drawbacks create huge legal uncertainties on determining the copyright liability of ISPs, such as online streaming issues. According to the Chinese legislation, these drawbacks shall be solved by the third amendment of the Copyright Law in the future.

d. The impact of the E-commerce law on ISPs

The legislative history of the ISP-relate provisions can be divided into three stages in China. First, before the E-commerce came into effect on January 1, 2019, the copyright liability of ISPs is generally regulated by the RPRD for trial implementation, while the Copyright Law and Tort Law merely stipulate several principles for ISPs. Second, after the E-commerce came into effect and before the new amendment of the Copyright law, most of the ISPs shall be regulated by the E-commerce law. However, the Internet content providers listed in Article 2 of the E-commerce law shall still be regulated under old provisions of ISPs. Third, after the new amendment of the Copyright law is promulgated, it shall provide a safe harbor for ISPs, but exclude Internet content providers from the safe harbor in order to strengthen online copyright protection. Therefore, the Third Amendment of the Copyright Law will provide an improved copyright liability system for ISPs, and cover the exception in Article 2 of the E-commerce law in the future.

A hypothetical "Star Wars" case is a good example to explain the impact of E-commerce law on the copyright liability of ISPs in China. The copyright owner of Star Wars sells authorized products over Amazon.com, publishes novels over Kindle E-books, streams songs over Amazon Music and streams movies over Amazon Video. On the first stage, before the E-commerce came into effect on January 1, 2019, all the copyright issues related to Star Wars over Amazon, Inc. shall be regulated under Copyright Law, Tort Law, the RPRD and the 2012

Provision.

On the second stage, after the E-commerce came into effect and before the new amendment of Copyright law, the copyright issues related to Star Wars on Amazon.com shall be covered under E-commerce law, while the remaining issues shall be covered by the old laws and regulations. For instance, an e-commerce business operator sold a backpack printed with a Star Wars image to a buyer through Amazon.com without authorization by the copyright owner. According to Article 42 of the E-commerce law, the copyright owner of can send a notification to Amazon.com, and request Amazon.com to delete, block, disconnect or terminate transactions and services.[264] If Amazon.com fail to take down the infringing backpack in time, it is jointly liable with the e-commerce business operator.[265] If copyright infringements related to Star Wars occur on Amazon Music, Amazon Video and Kindle E-books, the copyright owner shall seek remedies under the old laws and regulations.

On the third stage, after the new amendment of the Copyright law is promulgated, it shall definitely cover the exception in Article 2 of the E-commerce law. According to Article 73 of the Copyright draft, although Paragraph 1 stipulates that ISPs do not bear duty of examining copyright, Paragraph 5 provides that "it is not applicable to Paragraph 1 of this article if network service providers provide to the public the works, performances, or audio-visual recordings of others through information networks."[266] In other words, the Internet content providers shall actively examine the copyright content with copyright owners before providing them to the public. For example, Amazon, Inc. shall examine all the copyrighted works on Amazon Music, Amazon Video and Kindle E-books before dissemination. As a result,

[264] E-commerce Law, art. 42, para. 1: "If an intellectual property right holder believes that his intellectual property right has been infringed, he has the right to notify the relevant e-commerce platform operator to take necessary measures, such as deleting, blocking, disconnecting or terminating transactions and services."
[265] E-commerce Law, art. 42, para. 2: "In the case of failing to take necessary measures in a timely manner, the e-commerce platform operator and the online business operators concerned shall be jointly and severally liable for expanded part of the damage to the intellectual property right holder."
[266] 2014 Copyright Draft, *supra* note 30, art. 73.

if copyright infringements related to Star Wars occur on Amazon.com, the copyright owner should seek remedy under E-commerce law, the other copyright infringements shall be regulated under the Third Amendment of the Copyright Law in the future.

In sum, E-commerce law sets up a complete IP protection mechanism of ISPs, but also creates huge legal uncertainties on the copyright liability of Internet content providers. The Third Amendment of the Copyright law shall solve this problem and provide an improved copyright liability system for ISPs in the future. Before E-commerce law, people's courts highly rely on Tort Law, the RPRD and the 2012 provision when solving copyright infringement cases of ISPs in China. The specific cases will be addressed in Part C below.

C. Cases

Part C first presents the background on the differences of case law between the U.S. and China in Section 1, then examines recent cases of ISPs from China, with a special focus on the *SOHO* case in Section 3. Section 4 introduces the anti-unfair competition approach through the *Tencent* case. Section 5 concludes a summary on similarities and differences of ISP policies between the U.S. and China.

1. Background

Although case law is not binding in civil law countries such as China, it plays a more and more important role in Chinese judiciary. Generally, the primary people's courts have jurisdiction to hear local cases at first instance. A party may bring an appeal to the people's court at the next higher level, and the second instance is the last instance.[267] In 2014, China established three IP courts, and expanded a pilot program for specialized IP Courts to include four new IP tribunals in 2016.[268] IP Courts are specialized intermediate people's court, which

[267] *See* Organic Law of the People's Courts of the PRC, Chapter II art. 12 to 28.
[268] Office of the United States Trade Representative, 2017 Special 301 Report, at 7, available at https://ustr.gov/sites/default/files/301/2017%20Special%20301%20Report%20FINAL.PDF.

have jurisdiction to hear IP cases of first instance (e.g. patent) and IP cases of second instance that appealed from local primary people's courts.[269] According to the "Provisions of the Supreme People's Court on Case Guidance Work,"[270] the Supreme People's Court publishes "guiding cases" that the people's courts at all levels shall take them as reference when trying similar cases.[271] The guiding case should be effective and comply with several requirements: (1) such case arouses wide public concern; (2) case involves circumstances where relevant laws only stipulate principled provisions; (3) case that is typical to other case; and (4) case that involves difficult and complicated situations or new types of cases.[272] For guiding cases of IP, the Supreme People's Court selected cases from different IP courts as its research base on case guidance and precedent.[273]

This Part analyzes three cases of ISPs in China and compares them with the U.S. cases in Part A. These cases have similar facts and issues with the U.S. cases, but the people's courts adopt different approaches on the issues. In the first case *Baidu*,[274] the Beijing High People's court adopted the similar rationale from *YouTube*, but the difference is that it also imposed a duty of care on ISPs. The second *SOHO* case has a similar retransmission issue with *Aereo* and *VidAngel* case. Although the trial court adopted a similar approach from the U.S. case law, the Shanghai IP court rejected the trial court's approach and adopted a stricter duty of care requirement than in *Baidu*. The third case is a landmark case from the Supreme People's Court,

---

[269] Zui gao ren min fa yuan guan yu Beijing Shanghai Guangzhou zhi shi chan quan fa yuan shen an jian guang xia de gui ding (最高人民法院关于北京、上海、广州知识产权法院案件管辖的规定) [Provisions of the Supreme People's Court on the Jurisdictions over Cases by Intellectual Property Courts in Beijing, Shanghai and Guangzhou] (promulgated by the Supreme People's Court, Oct. 31, 2014, effective in Nov. 1, 2014) (China) Fa Shi No. 12 (2014) [法释(2014) 12 号], art. 1. Translated by Westlawchina (www.westlawchina.cn).

[270] Zu gao ren min fa yuan guan yu an li zhi dao gong zuo de gui ding (最高人民法院关于案例指导工作的规定) [Provisions of the Supreme People's Court on Case Guidance Work] (promulgated by the Sup. People's Ct., Nov. 26, 2010, effective Nov. 26, 2010) (China) Fa Fa No. 51 (2010) [法发(2010) 51 号]. Translated by Westlawchina (www.westlawchina.cn).

[271] Provisions of the Supreme People's Court on Case Guidance Work, *supra* note 270, art. 7.

[272] Provisions of the Supreme People's Court on Case Guidance Work, *supra* note 270, art. 2.

[273] Office of the United States Trade Representative, *supra* note 268, at 7.

[274] *Baidu*, Beijing High People's Ct. Aug. 5, 2014, *supra* note 147.

Tencent.[275] Although the facts in *Tencent* are similar with *Blizzard*, the Chinese technology giant Tencent filed an anti-unfair competition lawsuit instead of a copyright lawsuit. Section 4 analyzes why Chinese technology companies consider anti-unfair competition law as a more powerful weapon than copyright law, and Chapter IV examines this case in the trademark regime.

2. *China Youth Publishing Group (Beijing) v. Baidu Tech Ltd. (Shenzhen)*

a. Background

Baidu Wenku is a controversial online document-sharing service provided by the defendant, Baidu Technology Ltd. Baidu Wenku allows its users to share digital documents to the public for online reading. 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, the number of documents in Baidu Wenku's literature section decreased to 150. In September 2011, Baidu closed the literature section in Baidu Wenku.[276]

b. The trial court's decision

On December 1, 2011, Wan Juan, who is the author of the book "Kao's Diary," granted its exclusive right of dissemination via information network to the plaintiff, China Youth Publishing Group. Kao's Diary was a popular book and its sales were ranked 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

[275] *Tencent*, Sup. People's Ct. Feb 18, 2014, *supra* note 146.
[276] *Baidu*, at 2-3.

files of Kao's Diary can also be found on Baidu Wenku, which were uploaded by other Internet users from 2011 to 2012.[277] 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. Moreover, 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 actions of Baidu constituted joint-infringement of assistance. Therefore, Baidu bears appropriate compensation liability on plaintiff's lost.[278]

c. The appellate court's opinion

The appellate court, Beijing High People's Court, believed the main issue of this case is "whether the action that Baidu provided Kao's Diary in Baidu Wenku constituted direct infringement or joint-infringement."[279] Therefore, the court focused on analyzing two issues: (1) whether Baidu constituted direct-infringement; and (2) whether Baidu constituted joint-infringement of abetment or assistance.

i. Direct infringement

On whether Baidu constituted direct infringement, the court concluded that "the prerequisite of an ISP constituted direct-infringement is the existence of whether an ISP have the action that provided the work."[280] In other words, whether an ISP direct infringes copyright depend on whether it make the copyrighted work available online. In conclusion, the Beijing High People's Court agreed with trial court's decision that "Baidu Wenku qualifies the definition of information storage space (see the RPRD 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

[277] *Id.*
[278] *Id.* at 7.
[279] *Id.* at 19.
[280] *Id.* at 21.

constituted direct-infringement."[281]

ii. Joint-infringement

The appellate court also conclude a prerequisite for an ISP to bear joint-liability by its network users who used its service to implement infringing activities. Similar to the subjective standard in *YouTube*, on whether an ISP constitutes joint-infringement of abetment or assistance, the ISP shall have the subjective fault that it "knows or should have known the infringing activities."[282]

On determining whether an ISP is at fault, an ISP must 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 via information networks.[283] Thus, Article 9 of the 2012 Provision lists several factors on how to determine whether an ISP should have known an infringement was occurring. Based on these two rules, the appellate court analyzed whether Baidu was at subjective fault for 'knowing' or 'should have known' the infringing activities based on five factors from Article 9. This five-factor test is similar to the red flag test in *YouTube*, including similar rationale from the objective and subjective standard, and the something more standard. Notably, the Beijing High People's Court focused its analysis on the duty of care requirement, which is an active-preventive approach of ISPs. This section examines the red flag test[284] in Baidu below, which is called the "should have known" rule.[285]

iii. "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, whether Baidu had

[281] *Id.*
[282] *Id.* at 21-22.
[283] 2012 Provision, art. 8 para. 3.
[284] *Id.* at 15.
[285] *Id.* at 22.

subjective fault that it had constructive knowledge on Kao's Diary was a popular book, and therefore, adopt effective technical measures to prevent copyright infringement.[286] The appellate court concluded that even though the ISP knew the information of the book, the ISP should not implement key-word filters, such as the author or title of the book, in its information storage space. Adopting such technical measures is harmful to information communication and sharing because it might possibly limit the dissemination of the derivative work, such as comments, book review, or fair use of the book.[287]

Second, the appellate court analyzed whether Baidu "should have known" Kao' Dairy because it actively selected, classified, edited, and sorted out uploaded documents from its users.[288] The court concluded "the purpose of setting a 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 actually accessed the content of Kao's Diary."[289]

Third, the court analyzed whether Baidu directly obtained any economic benefit from its network users' uploading activities, therefore, constituting joint-infringement of abetment. Article 11 paragraph 1 of the 2012 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 towards such network user's act on infringement of the right of dissemination on information networks."[290]

According to paragraph 1, the court held that whether Baidu directly obtained any economic benefit from its network users' uploading activities is a factor to determine whether Baidu has a higher duty of care, not a prerequisite to determine whether Baidu's action constituted

---

[286] 2012 Provision, *supra* note 241, art. 9 item (2): "Type and popularity of the work, performance, and audiovisual recordings disseminated and the degree of the obviousness of the infringement."
[287] *Baidu,* at 22.
[288] 2012 Provision, art. 9 item (3): "Whether the ISP actively selects, edits, modifies, or recommends the works, performance, and audiovisual products."
[289] *Baidu*, at 23.
[290] 2012 Provision, art. 11 para. 2.

abetment joint-infringement.[291]

Article 11 paragraph 2 of the 2012 Provision stipulates that where a network service provider gains profits from placing advertisements into a specific work, it shall be determined that the network service provider directly obtains economic benefits. The court concluded 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."[292] Although Baidu obtained the right of use 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 economic benefits.[293]

Fourth, on whether the "points reward system" of Baidu Wenku constituted joint-infringement of abetment, the court concluded that "the point reward system is a business modal of Baidu 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 economic benefits."[294] Therefore, the points reward system did not indicate any subjective intention of abetment infringement.

Fifth, the court examined whether the number of hits on a document triggers duty of care requirement. According to Baidu, documents appear on the Baidu Wenku homepage's recommendation document section is because these documents were authorized by the copyright owners. Number of hits on a document is not a factor for its placement in the recommendation section. The court believed that (1) Baidu knew which documents were authorized by copyright owners; and (2) 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

[291] *Baidu*, at 24.
[292] *Id.*
[293] *Id.*
[294] *Id.*

quantity.[295] "However, from the first infringing document was uploaded on 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."[296] In other words, the Beijing High People's Court recognized duty of care as an affirmative obligation for ISPs, and therefore, Baidu has to adopt positive and reasonable measures to prevent infringement.[297]

Moreover, the appellate Court upheld the trial judgment that, "even Baidu pay normal duty of care in a standard of a reasonable person, it is easy to find that the possibility is extremely low for the related document to obtain authorization, therefore, it is highly possible that the related document might infringe copyright."[298] Furthermore, the court held that

> "when an information space service provider knows that related documents are not authorized by copyright owner and has been viewed massive amounts of times, it should bear a higher 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 measures to prevent infringement from happening or sustaining."[299]

This holding has the similar rationale with the something more standard in *YouTube*, and imposes a duty of care requirement based on Article 11 of the 2012 Provision.[300] The Chinese legislation also adopts the rationale from the duty of care requirement and enacts it into Article 41 of the E-commerce Law, which require ISPs to actively cooperate with copyright owners and adopt preventative measures to protect copyright.

In conclusion, the Beijing High People's Court's decision adopted a similar rule of thumb in *YouTube*, and developed them in the should have known rule. First, the court determined that Baidu subjectively knew the fact that the infringing document on its network

---

[295] *Id.* at 25.
[296] *Id.*
[297] 2012 Provision, art. 9 item (4): "Whether the ISP has taken positive and reasonable measures to prevent infringement."
[298] *Baidu*, at 25.
[299] *Id.*
[300] 2012 Provision, art. 11.

was popular and unauthorized. Second, the fact that the number of hits of the infringing document has reached a high quantity, which was objectively obvious for Baidu to pay a reasonable duty of care on the infringing document as a reasonable person.[301] Third, the appellate Court required that the ISP should actively censor the document and adopt effective measures to prevent infringement, which is similar to the something more standard in *YouTube*. However, there are differences between the duty of care requirement in *Baidu* and the something more standard in *YouTube*, which will be analyzed below.

iv. Duty of care requirement

The 2012 Provision has a unique duty of care requirement for ISPs, which does not exist in the U.S. Copyright Act. The duty of care requirement originated from Article 11 paragraph 1 of the 2012 Provision that require ISPs bear a higher duty of care when they directly gain economic benefits from their users' acts.[302] Based on the duty of care requirement, Article 8 paragraph 3 of the 2012 Provision requires ISPs to adopt "reasonable and effective technical measures" to "discover a network user's infringement."[303] However, the issue is that the 2012 Provision does not provide details on what constitutes reasonable and effective technical measures. Compared to the something more standard in *YouTube*, the duty of care requirement in *Baidu* has a similar rule of thumb. However, people's courts have higher requirements on the technical measures of ISPs.

Both the duty of care requirement in *Baidu* and the something more standard in *YouTube* require ISPs to take active steps to prevent copyright infringement on its network. Moreover, in both *Baidu* and *YouTube*, the ISPs adopt similar fingerprint systems as their technical measures to protect online copyright. However, in *Baidu*, although the defendant claimed that

[301] *Baidu*, at 25.
[302] 2012 Provision, *supra* note 241, art. 11 para. 2.
[303] 2012 Provision, art. 8 para. 3.

it had fulfilled its reasonable duty of care by adopting several technical measures, the people's courts disagreed. Similar to *YouTube*, Baidu's fingerprint system automatically compares uploaded files with Baidu's official copyright database. The fingerprint system blocks 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.[304] The trial court discussed this issue and believed that the fingerprint system functioned as a comparison of the copyright content's fingerprint, but the ISPs did not have access to obtain copyright content. Even though it was not appropriate to require the ISP to filter, block, or delete a file because of a famous work because such an obligation was also not beneficial for social development and cultural prosperity,[305] the trial court did not consider the fingerprint system to be a reasonable and effective technical measure for Baidu to fulfill the duty of care requirement. Instead, the trial court required ISPs to establish a verification mechanism when the number of hits of a copyright work reached a high quantity, and actively contact the copyright owners when the work involves copyright infringement.[306] The appellate court agreed and also required ISPs to actively contact the copyright owners and verify the potential infringing material.[307]

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

[304] *Baidu*, at 16.
[305] *Id.* at 5-6.
[306] *Id.* at 7.
[307] *Id.* at 25.

copyright work.

However, the fingerprint of a digital file is not the same as a human being's fingerprint. A human being is not able to change its fingerprint easily, 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 a genuine copyright work, with almost the same content. Therefore, the fingerprint of a digital file is similar to an identification code. Each digital file has its own unique identification number, unless it is the exact copy of a digital file. Even two very similar digital files with only slight them have different identification codes.

Moreover, 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 "Star Wars" movie to a cloud sever without the copyright owner's authorization, the ISP may cooperate with the copyright owner of the movie and obtain the fingerprint of the file. As a result, 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, or a MP4 file can be modified to AVI file, or the video quality of 1080P can be modified to 720P. A little modification 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.

In conclusion, people's courts held that merely implementing the fingerprint system is not a reasonable and effective technical measure for an ISP to fulfill duty of care requirement, and indicated that ISPs should actively cooperate with the copyright owners to verify the potential infringing material. To clarify how ISPs should act in order to fulfill duty of care requirement, the new promulgated E-commerce law adopts the experience in *Baidu* and

provides a statutory scheme. Article 41 requires ISPs to formulate IPR protection rules and cooperate with IPR holders.[308] In addition, Article 43 adopts the rationale from *Baidu*, which establishes a N&T system and requires ISPs to actively inform the IP holders "that a complaint may be filed with the relevant competent department or a lawsuit filed with the people's court."[309] Therefore, duty of care requirement imposes an affirmative duty on ISPs in China. To fulfill this requirement, ISPs should follow Article 41 to 45 E-commerce law to actively cooperate with IP owners and set up IP protection system.

3. *TV.SOHO.COM (Tianjin) v. Shanghai Hode Information Technology Co. Ltd.*

This section first presents the *TV.SOHO.COM v. Shanghai Hode Information Technology Co. Ltd.* case (hereinafter "*SOHO*"),[310] then compares *SOHO* with *Aereo*, *VidAngel* and *Baidu* in order to conclude the different approaches to the issues of ISPs among different courts.

a. Background

The *SOHO* case was chosen as a typical case in "Shanghai Intellectual Property Court Judgments Selection."[311] Shanghai IP Court was established in 2014 as one of the specialized IP courts in China. The plaintiff-appellee SOHO owns the exclusive rights of two TV programs "Zhang" and "Xing". In 2014, SOHO found the defendant-appellant Hode provided online broadcasting of the TV programs without its authorization on Hode's website "Bilibili." SOHO filed a lawsuit against Hode in Shanghai Pudong New Area People's Court, and requested that

---

[308] E-commerce Law, art. 41.
[309] E-commerce Law, art. 43, para. 2.
[310] Fei hu xin xi ji shu (tian jin) you xian gong si su shang hai huan dian xin xi ke ji you xian gong si qin hai zuo pin xin xi wang luo chuan bo quan jiu fen shang su an [飞狐信息技术(天津)有限公司诉上海幻电信息科技有限公司侵害作品信息网络传播权纠纷上诉案] [*TV.SOHO.COM (Tianjin) v. Shanghai Hode Information Technology Co. Ltd.*], Shanghai IP Ct. (上海知识产权法院) Mar 25, 2016] (2015) Hu Zhi Min Zhong Zi No. 276 [(2015)沪知民终字第 276 号] (China) [hereinafter *SOHO*].
[311] SHANGHAI INTELLECTUAL PROPERTY COURT (上海知识产权法院), SHANGHAI INTELLECTUAL PROPERTY COURT JUDGMENTS SELECTION (2015-2016) [上海知识产权法院裁判文书精选 (2015-2016)] [Wang Qiuliang (王秋良) et al. eds., Global Tone Communication Technology (Shanghai) Co. Ltd. [中译语通信息科技(上海)有限公司] trans. Intellectual Property Press (知识产权出版社) 2018].

Hode should stop the infringement immediately. Hode argued that these two TV programs were not stored on Bilibili's server because they were broadcasted on Bilibili via the links uploaded by its users.[312]

b. Hode's deep link technology

Bilibili is a bullet-screen video website that allows its users to contribute videos from other websites to Bilibili. The process is that a user copies the Uniform Resource Locator (URL) of a VOD webpage and sends it to Bilibili's submission webpage. Bilibili's server will send a request to the server of the VOD website for extracting the video file data. After the video is captured by Hode's deep link technology, it could be played in Bilibili's web player. Users could comment the video and the comments would be scrolled as bullets on the screen.[313] Thus, the deep link technology allows user to watch and comment VOD from different websites on Bilibili.

c. The trial court's decision

The trial court held that Hode infringed the right of dissemination via information network of SOHO, and its rule of thumb was similar to *Aereo*. In *Aereo*, the U.S. Supreme Court considered Aereo's technology were substantially similar to the CATV and performed plaintiff's copyrighted works publicly, therefore, infringed on then public performance right.[314] The trial court adopted a similar rationale from *Aereo* by reasoning: (1) Bilibili substituted linked websites to disseminate copyrighted works; and (2) Hode made artificial interventions to provide the TV programs without authorization. Moreover, on the issue of whether Hode's deep link technology committed infringement, the trial court analyzed in three perspectives.

First, for the interest of copyright owners, the court believed that Hode's deep link technology was far beyond the traditional link technology that helps users to locate information,

---

312 *SOHO*, Shanghai IP Ct., *supra* note 310, at 1. *See also* SHANGHAI IP COURT, *supra* note 311, at 531.
313 *SOHO,* at 3-4. *See also* SHANGHAI IP COURT, *supra* note 311, at 533-544.
314 *Aereo,* at 1206-1210.

but it allows users watch video selectively and directly on Bilibili without visiting the linked website. Even if Hode provides technical guide to users to visit the linked website, it still commits infringement. Second, for the interests of ISPs, Hode obtained economic benefits by disseminating works to the public as its own without paying any royalties, which damaged the interests of linked ISPs, and therefore, was illegitimate. Third, for the public interests, Hode provided copyrighted works in lieu of the linked ISPs, which damaged the interests of the copyright owners and ISPs that legally obtained licenses.[315]

d. The appellate court's decision

The appellate court, Shanghai IP court, reversed the trial court's decision by holding that "Hode shall not be liable for direct infringement."[316] The appellate court disagreed with trial court's reasoning that Bilibili substituted linked websites to disseminate copyrighted works. Moreover, the court also disagreed with the trial court's reasoning from the perception of copyright owners, ISPs and the general public, which was beyond the scope of right of dissemination via information network. Instead, it analyzed whether Bilibili infringed SOHO's right of dissemination via information network based on the secondary copyright infringement theory. As a conclusion, the court held that Hode should have subjectively known the infringement, therefore, was liable for joint infringement as it failed to perform the duty of care.

i. Right of dissemination via information network

The appellate court first discussed whether Hode's deep link service infringed SOHO's right of dissemination via information network. According to Article 3 of the 2012 Provision, anyone who makes copyrighted works available on the information network without authorization infringes a copyright owner's right of dissemination via information network.[317]

---

[315] *SOHO*, at 5. *See also* SHANGHAI IP COURT, *supra* note 311, at 535.
[316] *SOHO*, at 9. *See also* SHANGHAI IP COURT, *supra* note 311, at 539.
[317] 2012 Provision, art. 3: "Any web user or web service provider who makes any works, performance or audio-video product, for which others have the right of dissemination through information networks, available on any

Thus, whether a person who commits such infringement shall bear direct infringement liability depends on whether the copyrighted works were placed on the information network. Notably, the court pointed out that "placing works on the information network" was a matter of fact, and the fact shall refer to "the initial act of placing works on information network."[318] In this case, two TV programs of SOHO were initially provided by other ISPs. Bilibili merely linked the video files from other websites to its own website for online playback. Therefore, Bilibili should be regarded as network link service rather than the ISPs that place the works on the information network."[319]

Compare *SOHO* to *Aereo* and *VidAngel*, all these cases share a similar issue: whether an ISP can retransmit copyrighted works through the network without authorization. Although the ISPs of these cases adopted different network technologies to retransmit copyrighted works, all the courts focused on whether such retransition infringes copyright owner's exclusive rights. In the U.S., the main issue is whether ISPs infringe on public performance rights. In China, the main issue is whether ISPs infringe on the right of dissemination via information network. In *SOHO*, although the trial court's approach to the issue is similar to the approaches in *Aereo* and *VidAngel*, the Shanghai IP court did not follow this approach. In fact, Shanghai IP court adopted a secondary copyright infringement theory of ISPs, which is similar to the approach in *YouTube*.

ii. Contributory infringement

Although the Shanghai IP court decided that Hode's act did not infringe on the right of

information network without authorization shall be decided by the people's courts to have infringed upon the right of dissemination through information networks unless otherwise provided in laws or administrative regulations.
Whoever uploads any works, performance or audio-video product to any web server, sets it as shared file, or uses file sharing software or other ways to make it available on any information network so that the public can download, browse or otherwise access it at such time and place chosen by them in their discretion shall be decided by the people's courts to have committed the behavior specified in the preceding paragraph."

[318] *SOHO*, at 8-9. *See also* SHANGHAI IP COURT, *supra* note 311, at 538-539.

[319] *Id.*

dissemination via information network directly, whether Bilibili should be liable for indirect infringement remained an issue. Because Bilibili contributed to the dissemination of the copyrighted contents from the linked websites, it was likely to commit contributory infringement under Article 36 of the Tort Law and Article 7 of the 2012 Provision. The appellate court concluded that whether an ISP should be liable for contributory infringement depends on whether the ISP infringed on the right of dissemination via information network. For link service providers such as Hode, whether Bilibili infringed the right of dissemination via information network depends on whether the contents on the linked websites were disseminated without the permission of the copyright owners.[320]

In this case, for one of SOHO's TV programs "Xing," it was licensed to Tencent Video (v.qq.com) and remained valid through the time of infringement. Thus, Bilibili should not be deemed to commit indirect infringement by linking a legitimate video. For the other SOHO TV program "Zhang," it was licensed to LeTV (www.le.com) before but expired by the time of infringement. As a result, the court recognized that "Zhang" was disseminated on the linked website without SOHO's authorization. Whether Bilibili committed secondary infringement depends on whether Hode knew or should have known such video was disseminated without authorization.[321]

iii. "Should have known" rule

Different from the five-factor test in *Baidu*, a three-factor test was adopted by the Shanghai IP court to determine whether Hode should have known that "Zhang" was disseminated without authorization. First, the court analyzed the economic benefits of Hode's deep link service. On the one hand, Bilibili provided users with more targeted guidance and increased royalty to linked websites, thus, bringing more economic benefits to Hode. On the

[320] *SOHO*, at 9. *See also* SHANGHAI IP COURT, *supra* note 311, at 539.
[321] *Id*, at 9-10.

other hand, Bilibili caused more damage to the copyright owners if the video of linked websites constituted infringement. Second, the court recognized that Bilibili was providing oriented link services rather than passive site-linking service. In other words, Hode technically controlled the contribution information from its users and screened links for certain websites. Third, for the linked contents, the court believed that TV programs and movies were different from other copyrighted works. The copyright owners of TV programs and movies would only grant authorizations to certain legitimate ISPs in China. For example, the copyright owner of a new released "Star Wars" movie will probably only grant authorization to Netflix or Amazon Movie. Therefore, oriented link service providers were required to be familiar with these legitimate ISPs and their contents. There was no excessive burden for oriented link service providers to provide the links to these legitimate websites as much as possible.[322]

In summary, the Shanghai IP court concluded that Hode should bear reasonable duty of exercising higher level care on the legality of the dissemination of the linked.[323] Thus, Hode should know if the linked contents were disseminated under authorization. The appellate court held that Hode was liable for joint infringement as it failed to perform the duty of care to censor the linked contents.

iv. Duty of care requirement

The issue in *SOHO* is whether the Shanghai IP court construed the duty of care requirement appropriately. According to Article 11 paragraph 1 of the 2012 Provision, when an ISP gains economic benefits directly from works provided by a network user, the ISP has a "higher duty of care"[324] towards the network user's act because such act may infringe the right of dissemination via information networks. However, the criterion of "higher duty of care" is

[322] *SOHO*, at 10. *See also* SHANGHAI IP COURT, *supra* note 311, at 540.
[323] *Id*, at 10-11.
[324] 2012 Provision, art 11 para. 1.

unclear under the 2012 Provision. Thus, the criterion of duty of care requirement in different people's courts are different. Compared to *Baidu*, the Shanghai IP court construed ISPs' duty of care strictly, which may put too much burden on link service providers.

The appellate court believed that the burden for link service providers to recognize and provide links to legitimate ISPs was not excessive. However, it would be too much burden for link service providers to censor if each copyright work from a legitimate ISP is still under authorization. It is the Internet content providers' duty to assure their contents are legitimate, not link service providers. In this case, Hode had the duty of care to assure that its users contributed legitimate information to Bilibili. Thus, Hode technically controlled the linked websites to certain legitimate ISPs. However, according to Shanghai IP court's rationale, even though linked websites come from legitimate ISPs, Hode still bears the duty of exercising care on whether the linked contents are legitimate.

According to the facts in this case, LeTV was authorized by SOHO to play its TV program "Zhang," therefore, LeTV was responsible to remove "Zhang" from its website when the license was expired. If LeTV removes the original URL of "Zhang," the link on Bilibili would become invalid. However, neither LeTV removed "Zhang" from its website nor SOHO notified LeTV to remove "Zhang."

On the contrary, Hode expeditiously deleted the link to "Zhang" after receiving the notification from SOHO. If Hode provided "Zhang" on Bilibili and removed it immediately after receiving the notification, Hode shall be exempted from secondary copyright liability based on the safe harbor doctrine. Because LeTV provided "Zhang" and did not remove it after the license expired, Hode was liable for joint-infringement. As an ISP, LeTV bears the duty of care to provide legitimate contents. However, as an ISP to provide link service, whether Hode bears the duty of care to censor each linked content from legitimate ISPs is questionable.

Compared to duty of care requirement in *Baidu*, the Shanghai IP court placed a heavier

duty of care requirement on ISPs. In *Baidu*, the Beijing High People's court ruled that an ISP should pay higher duty of care than a reasonable person.[325] For instance, when watching the Star Wars movie from genuine ISPs, such as Netflix or Amazon Video, a reasonable person may assume that such ISPs are authorized by the copyright owner to broadcast the movie. A reasonable person will not contact the copyright owner to verify the authorization. In *SOHO*, Hode provided link services to legitimate ISPs because it assumed that contents from these ISPs were under authorization. Therefore, Hode fulfills the duty of care requirement under *Baidu* because it pays higher duty of care than a reasonable person. Nonetheless, there is no criterion on what extent of duty of care should an ISP bear in China. Although the Shanghai IP court believed that "there was no excessive burden" for link service providers to provide the links from legitimate ISPs,[326] the burden for Internet link providers to censor each linked content is excessive.

e. Paradox for ISPs

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 the Safe Harbor doctrine and the N&T 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.[327] However, both the copyright owners and Chinese legislation demand ISPs 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

[325] *Baidu*, at 23.
[326] *Id.*, at 10.
[327] JEREMY & CHRISTOPHER, *supra* note 2, at 405.

has proactively taken reasonable measures to prevent infringement."[328] Such paradoxical arrangement requires ISP to act both actively and passively on copyright protection, which is unsustainable under the current online environment.[329]

This paradox appeared both in *Baidu* and *SOHO*. In *Baidu*, neither the trial court nor Appellate court mentioned Article 8 paragraph 2 of the 2012 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."[330] However, after holding that Baidu should pay duty of care on the number of hits on Kao's diary, the Beijing High People's court required that the ISP should actively try to contact the uploader and verify if the related documents are the original or under legal authorization. Moreover, the court also required that the ISP should adopt effective measures to prevent infringement from happening or continuing. As a result, the 2012 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 issue: whether an ISP should actively involve in copyright protection.

In *SOHO*, the level of duty of care requirement was higher than in *Baidu*. Hode was not allowed to stay passive even though it only provided links to certain legitimate ISPs. The Shanghai IP court ruled that link service providers should bear reasonable duty of exercising higher level of care on whether the linked contents were disseminated legally. In conclusion, even though the 2012 Provision does not require ISPs to conduct proactive examination on its network, the Chinese People's courts tends to push ISPs to actively protect copyright by adopting a strict duty of care requirement.

---

[328] 2012 Provision, *supra* note 241, art. 9 (iv).
[329] JEREMY & CHRISTOPHER, *supra* note 32, at 405.
[330] 2012 Provision, *supra* note 241, art 8.

f. An active-preventive approach to ISPs

Both the Chinese legislature and case law show the trend that China is shifting from a passive-reactive approach towards an active-preventive approach to ISPs. Since 2010, the Chinese legislation started to adopt ISP-related principles from the U.S. Copyright Act and case law, and enacted these principles into different Chinese laws and regulations for trial implementation. Because the DMCA adopted a passive-reactive approach to ISPs, such as the safe harbor doctrine, China also adopted the same approach. However, with the development of Chinese online market, the Chinese legislation began to adopt an active-preventive approach to ISPs in order to regulate its biggest online market in the world. Moreover, the duty of care requirement was enacted in the 2012 Provision, and the Chinese People's courts tends to apply it strictly.

In addition, the Chinese legislation adopted the active-preventive approach to ISPs and began to implement it into new laws. The new promulgated E-commerce law adopted the rationale from the duty of care requirement by stipulating that ISPs shall "formulate intellectual property right protection rules, and strengthen cooperation with intellectual property rights holders."[331] Moreover, the ongoing third amendment of the Copyright Law adopted an active-preventive approach to ISPs. For example, Article 73 Paragraph 1 of the Copyright draft provides a safe harbor for ISPs that provide storage, link or search services from the duty of examining copyright.[332] However, Paragraph 5 exempts Internet content providers from the Safe Harbor by stipulating that "it is not applicable to Paragraph 1 of this article if network service providers provide to the public the works, performances, or audio-visual recordings of others through information networks."[333] In other words, Internet content providers bear the duty of care to actively examine the copyright content before providing them to the public.

[331] E-commerce Law, art 41.
[332] 2014 Copyright Draft, *supra* note 30, art. 73, para. 1.
[333] 2014 Copyright Draft, *supra* note 30, art. 73, para. 5.

Therefore, the Chinese legislation is considering an active-preventive approach to Internet content providers.

4. *Beijing Qihoo Tech Ltd. v. Beijing Tencent Tech Ltd.*

This section first presents *Tencent* case, then compares it with *Blizzard* in order to explain the different approach on the issue of unauthorized third-party software between China and the U.S.

a. Background

Tencent begun with an influential incident, "3Q battle," and was highly publicized in 2010.[334] Defendant-appellant Qihoo Ltd. (hereinafter "Qihoo"), producer of anti-virus software "360 Safeguard," created an optimization software "360 Koukou Bodyguard" (hereinafter "Koukou") in 2010. Plaintiff-appellee Tencent Ltd. (hereinafter "Tencent") is the owner of the popular social software "QQ" that had almost 0.65 billion users in 2011.[335] Qihoo released Koukou on its website and advertised that Koukou can optimize QQ, such as removing advertisements from QQ, accelerating QQ's speed of service and improving QQ's privacy safety.[336] Within three days, more than 10 million users downloaded Koukou.[337] To counter Koukou, Tencent updated QQ that blocked itself from running on devices with Koukou installed. As a result, users were forced to choose sides, either to uninstall QQ or Koukou.[338]

On the issue of whether Qihoo specifically developed Koukou for QQ, and therefore, damaged the safety and integrity of QQ software, the Supreme People's Court recognized the fact that after operating Koukou, the User Interface (UI) of QQ's safety center was replaced by the UI of Koukou, and part of QQ software such as advertisement module stopped

[334] See https://en.wikipedia.org/wiki/360_v._Tencent.
[335] *Tencent*, *supra* note 146, at 40.
[336] *Tencent*, at 3.
[337] *Id.*, at 30.
[338] *Id.*, at 5.

functioning.[339] Therefore, the Supreme People's Court held that Qihoo actively induced and facilitated users to modify QQ's software, which constituted unfair competition.

b. A different approach with *Blizzard*

Because of the different legal environment between the U.S. and China, ISPs adopted different approaches on the issue of unauthorized third-party software. For ISPs, unauthorized third-party software assists their users in gaining unfair benefits, which is harmful for their businesses. In the U.S., ISPs tends to solve the issue of unauthorized third-party software under copyright law. For example, in *Blizzard*, the facts are similar with the facts in *Tencent*, but the difference is that two parties raise the issues under secondary copyright infringements and anticircumvention provisions. In *Blizzard*, MDY developed unauthorized third-party software, Glider, for Blizzard's game, WoW. To counter Glider, Blizzard updated WoW by launching TPM Warden. However, MDY also updated Glider to circumvent Warden. As a result, the court held that MDY did not constitute copyright infringement, but violated anticircumvention provisions of the DMCA.

On the contrary, in *Tencent*, Tencent did not follow *Blizzard*. As the copyright and trademark owners of QQ, Tencent claimed that Koukou induced its users to modify its QQ software without authorization and damaged QQ's goodwill.[340] However, rather than filing a lawsuit against Qihoo under copyright or trademark infringement, Tencent file a lawsuit under the old Anti-unfair Competition Law of the PRC (hereinafter "1993 Anti-unfair Competition Law").[341]

There are two main reasons why Tencent chose anti-unfair competition rather than copyright law in 2010. First, because China follows the U.S. approach on the secondary

---

[339] *Tencent*, at 56.
[340] *Id*.
[341] Fan bu zheng dang jing zheng fa (反不正当竞争法), Anti-unfair Competition Law of the PRC, promulgated by the Standing Comm. Nat'l People's Cong., Sep. 2, 1993, effective in Dec. 1, 1993 (China). Translated by Westlawchina (www.westlawchina.cn) [hereinafter 1993 Anti-unfair Competition Law].

copyright infringement theory of ISPs, it is likely that the People's court may follow *Blizzard* and rule against Tencent. In *Blizzard*, although Blizzard claimed that Glider constituted secondary copyright infringement, the Second Circuit held that "WoW players do not commit copyright infringement by using Glider ... MDY is thus not liable for secondary copyright infringement." [342] If Tencent files a lawsuit against Qihoo under secondary copyright infringement, it is likely that the People's court may follow *Blizzard* and hold that QQ users do not commit copyright infringement by using Koukou, therefore, Qihoo is not liable for secondary copyright infringement.

Second, the 2010 Copyright Law is unclear on defining TPM. Although Article 46 Item (6) of the 2010 Copyright Law prevents anyone from intentionally circumventing or destroying the technological measures applied by the copyright owner without the authorization,[343] the 2010 Copyright Law does not provide a definition of "technological measures." Thus, if Tencent follows *Blizzard* and develops a TPM like "Warden" to prevent QQ from Koukou, it is unclear whether such TPM is covered under the Copyright Law. Under this circumstance, Tencent adopted an anti-unfair competition approach instead of copyright law approach to the issue of unauthorized third-party software. Moreover, because *Tencent* was an influential case, ISPs in China tends to follow this anti-unfair competition approach to solve the issue of unauthorized third-party software.[344] As a result, China did not follow the anticircumvention approach in *Blizzard*, but developed an anti-unfair competition approach to the issue of unauthorized third-party software. Because this Chapter focuses on copyright, the anti-unfair competition approach will be examined in detail in Chapter IV.

---

[342] *Blizzard II*, 629 F. 3d, at 941.
[343] 2010 Copyright Law, art. 48 item (6).
[344] *See e.g.* Shanghai Synacast Media Technology Co., Ltd. v. Shanghai Damo Network Technology Co., Ltd., Shanghai Intellectual Property Court (2016) Hu No. 73 Min Zhong No. 34.

c. The development of the definition of "technological measures"

Because the lack of definition of technological measure created huge legal uncertainties in Copyright Law, three years after the 3Q battle, the RPRD provided a definition for "technological measure" in 2013. As mentioned before in Part B, Article 26 Paragraph 2 of the RPRD defines "technological measure" as any effective technology used to prevent or restrict browsing, enjoyment, or the availability to the public via an information network of a work.[345] Moreover, the Chinese legislation intends to amend this definition and enact it into the third amendment of the Copyright Law. According to Article 68 of the Draft of the third amendment of the Copyright Law, "Technological Protection Measure" means any effective technology, device or component used by right holders, to prevent or restrict their works from reproduction, browsing, enjoyment, operation, adaption or dissemination via network.[346] The scope of this new definition of TPM is broader than the one in the RPRD, and it protects the operation of software from unauthorized third-party software.

In conclusion, although the Chinses legislation may define TPM broader in the Third Amendment of the Copyright Law, current Copyright Law provides limited protection against unauthorized third-party software. After *Tencent*, China developed an anti-unfair competition approach to the issue of unauthorized third-party software.

5. Summary

In sum, most of the people's courts follows the U.S. approach on the secondary copyright infringement theory of ISPs. On some issues of ISPs, people's courts also developed different approaches such as the duty of care requirement. With the development of network

[345] RPRD, art. 26 para. 2: "Technological measure shall mean any effective technology, device or component used to prevent or restrict the browsing or enjoyment of a work, performance, or sound or visual recording that is not authorized by the right owner or the making available to the public via an information network of a work, performance, or sound or visual recording."

[346] 2014 Copyright Draft, *supra* note 30, art. 73, para. 5: "Technological Protection Measure" mentioned in this law, shall mean any effective technology, device or component used by right holders, to prevent or restrict their works, performance, audiovisual recordings, radio or television programs from reproduction, browsing, enjoyment, operation, adaption or dissemination via network."

technology and the wave of Web 2.0, it is no longer reasonable to require ISPs to keep purely passive on copyright protection, and they should be allowed to conduct certain management on the UGC.[347] As a result, China is shifting from a passive-reactive approach to an active-preventive approach to ISPs and establishing its own ISPs system with new laws. Because the new promulgated E-commerce law set up a legal foundation for the Chinese legislation to build its own active-preventive system of ISPs, it is likely that the Chinese legislation will establish an active-preventive system of ISPs in the Third Amendment of Copyright Law in the future.

[347] WANG, *supra* note 250, at 70.

Chapter IV: Secondary Trademark Liability of ISPs

This Chapter introduces recent development of ISPs' secondary liability in the trademark regime and discusses different approaches to online trademark infringement. Part A introduces the background of secondary trademark liability of ISPs and China's unfair competition approach of ISPs. Part B traces the development of secondary trademark liability of ISPs and analyzes several trademark cases of ISPs in the U.S. Part C introduces the new development of secondary trademark liability of ISPs in China, and examines the unfair competition approach to the secondary trademark liability of ISPs before the E-commerce Law. Section D analyzes a trademark case of ISPs and compares it to cases in the U.S. Part E analyzes the impact of new laws to the secondary trademark issues in China.

A. Introduction

In the digital age, ISPs are facing secondary trademark infringement issues as intermediaries, which are similar to the secondary copyright infringement issues of ISPs in Chapter III. When it comes to venues for online trademark infringement, there was a time when nothing could compete with ISPs such as eBay or Alibaba's Taobao. Traditionally, ISPs that provide e-commerce platforms are places to buy and sell goods. But in the 2000s, e-commerce platform also became places to buy and sell unauthorized counterfeit goods. Compared to the flea market, it is easier for an online business operator to sell counterfeit goods over e-commerce platforms. As a result, trademark counterfeiting has become a serious trademark infringement issue for ISPs, just like online piracy is a serious copyright issue for ISPs.

The legal issues of ISPs raised by e-commerce platform infringement are contentious nowadays. Online sellers of counterfeit goods were obviously guilty of trademark infringement. But regarding the firms and individuals that owned implicated markets, whether they are also

liable for secondary trademark infringement is controversial. From one perspective, ISPs are not liable because they do nothing more than create an online platform where buyers and sellers can interact. However, ISPs benefit from infringement in that affordable products are part of what brings buyers and sellers to the platforms. Moreover, the owners of ISPs likely could have done more to clamp down on unlawful behaviors, such as screening vendors more aggressively or performing censorship system.

Today, the ISPs are still significant battlegrounds for trademark law, but the same basic legal question continues to loom: how far should trademark liability extend beyond any direct lawbreakers? Both China and the U.S. adopt an approach that is similar to the secondary copyright liability of ISPs, but in different ways. In the U.S., because Congress did not enact a DMCA-like safe harbor in the Lanham Act to limit the secondary trademark liability of ISPs, this issue is addressed under case law.

It is not rare that courts in the U.S. borrow doctrines from one IP regime and apply them in other IP regimes.[348] Before the digital age, the U.S. courts developed the secondary trademark liability theory from tort law, such as contributory and vicarious liability theories. When the secondary trademark issue involves ISPs, courts applied similar rationale from secondary copyright liability of ISPs to solve secondary trademark issue. However, whether imposing secondary trademark liability that is similar to secondary copyright liability, and establishing a DMCA-like safe harbor for trademark law is appropriate for ISPs remain an issue. As a result, compared to the secondary copyright liability of ISPs, the law on secondary trademark liability of ISPs is undeveloped because the doctrine of secondary trademark liability is created by case law.[349]

In China, there was a time when the law governing secondary trademark liability of

[348] In *Sony*, the U.S. Supreme Court borrowed a staple article of commerce doctrine from the U.S. Patent Law. *See also* Chapter III Part I Section 1 Subsection b Paragraph iii-iv.
[349] Elizabeth K. Levin, *A Safe Harbor for Trademark: Reevaluating Secondary Trademark Liability after Tiffany v. eBay*, 24 BERKELEY TECH. L.J. 491, at 517 (2009).

ISPs is undeveloped. Similar to the secondary copyright liability of ISPs, the People's courts relied on the Joint-Liability theory of ISPs in Article 36 of the Tort Liability Law to solve the online trademark disputes of ISPs.[350] However, unlike the secondary copyright liability of ISPs that has additional legal materials such as the RPRD and the 2012 Provision, neither Chinese legislation stipulates regulation nor the Supreme People's Court provides judicial interpretation to the secondary trademark liability of ISPs. Therefore, for secondary trademark infringement issues of ISPs, merely one article in the Tort Liability Law is not enough. Because the Trademark law and the Tort Law did not provide enough remedy for secondary trademark infringement issues of ISPs, the trademark owners in China, especially tech companies, tend to request remedy under the 1993 Anti-unfair Competition Law instead of IP law or Tort law after *Tencent* in 2011.

In 2018, the uncertainties of the secondary trademark liability of ISPs were improved because a unified IPR protection system of ISPs was established in the E-commerce Law.[351] Not only did the E-commerce law adopt the safe harbor doctrine and the N&T system from the DMCA, but also expand the protection scope from merely copyright to all IP rights. However, whether a DMCA-like system that is designed for copyright protection can effectively protect trademark in China is questionable.

In this chapter, the discussion focuses on when secondary trademark liability of ISPs should be used to increase compliance with the law. The argument in favor of liability is that ISPs are often in a good position to discourage trademark infringement either by monitoring direct infringers or by redesigning their technologies to make infringement more difficult. The argument against is that legal liability almost inevitably interferes with the legitimate use of implicated tools, services, and venues. As a result, how to balance the interest among trademark

[350] *See e.g. E. LAND Ltd. v. Taobao Network Ltd.*, Shanghai First Intermediate People's Court (2011) Hu Yi Zhong Min Wu (Zhi) Zhong Zi No. 40.
[351] E-commerce Law, art. 41-45.

owners, ISPs and users remains an issue. In both China and the U.S., courts adopted a DMCA-like approach to the secondary trademark liability of ISPs. Moreover, the Chinese legislation adopted the anti-unfair competition from *Tencent* and developed this approach in the new promulgated Anti-unfair Competition Law of the PRC (hereinafter "2017 Anti-unfair Competition Law").[352] After comparatively analyzing these approaches, this chapter discusses whether a Block Injunction system of trademark is feasible in China.

B. Secondary trademark liability of ISPs in the U.S.

This part briefly introduces the trademark safe harbor provisions in the Lanham Act, then presents the development of secondary trademark liability of ISPs from case law, with a specific focus on examining *eBay*.[353]

1. Statute

Section 32(2)[354] of the Lanham Act creates a form of safe harbor from trademark infringement for "publisher[s] or distributor[s]."[355] However, this trademark safe harbor is less well-known than the copyright safe harbor in the DMCA. In addition, compared to the copyright law, the law on secondary liability of ISPs for online trademark infringement is

[352] Fan bu zheng dang jing zheng fa (反不正当竞争法), Anti-unfair Competition Law of the PRC, promulgated by the Standing Comm. Nat'l People's Cong., Nov 4, 2017, effective Jun 1, 2018. The English translation is available at http://app.westlawchina.com/maf/china/app/document?&docguid=i000000000000015f8f53025031a9a48c&hitguid=i000000000000015f8f53025031a9a48c&srguid=i0ad82b44000001656e7360b8adb8776f&spos=1&epos=1&td=53&crumb-action=append&context=3&lang=en. Translated by Westlawchina (www.westlawchina.cn) [hereinafter 2017 Anti-unfair Competition Law].

[353] *Tiffany (NJ) Inc. v. eBay Inc.*, 600 F.3d 93 (2d Cir. 2010).

[354] 15 U.S.C.§1114(2)(B)-(C).

[355] 15 U.S.C.§1114(2)(B): "Where the infringement or violation complained of is contained in or is part of paid advertising matter in a newspaper, magazine, or other similar periodical or in an electronic communication as defined in section 2510(12) of Title 18, the remedies of the owner of the right infringed or person bringing the action under section 1125(a) of this title as against the publisher or distributor of such newspaper, magazine, or other similar periodical or electronic communication shall be limited to an injunction against the presentation of such advertising matter in future issues of such newspapers, magazines, or other similar periodicals or in future transmissions of such electronic communications. The limitations of this subparagraph shall apply only to innocent infringers and innocent violators."

undeveloped.[356] First, unlike Section 512(k) of the DMCA that provides a definition for ISPs, Section 32(2) of the Lanham Act does not specifically apply to ISPs. It applies to publishers or distributors of "electronic communication,"[357] which extends the definition of publishers to online providers of content written by another.[358] Second, unlike Section 512(a)-(d) of the DMCA that provides safe harbor exemptions for different categories of ISPs, Section 32(2) of the Lanham Act only provides exemptions for some ISPs that are "innocent infringers,"[359] a term that is not defined in the Lanham Act. Third, Section 32(2) of the Lanham Act only exempts qualified ISPs from damages liability, and also from liability for injunctive relief in circumstances where an injunction would interfere with the normal operations of the ISPs.[360] In conclusion, although Section 32(2) of the Lanham Act provides trademark safe harbor provisions, the scope of this exemption is narrow and has rarely been applied by the court.[361]

2. Case law

This section examines two cases about secondary trademark liability of ISPs. *Hendrickson*[362] shows how the court applied Section 32(2) of the Lanham Act for ISPs. *eBay*[363] shows how the court applied similar rationale from secondary copyright liability theory of ISPs to solve the secondary trademark issues of ISPs.

a. Hendrickson v. eBay

In *Hendrickson*, the defendant eBay. Inc ("eBay") provides a popular Internet auction web service that allows sellers to post advertisements and buyers to bid for items they wish to

---

[356] Elizabeth K. Levin, *A Safe Harbor for Trademark: Reevaluating Secondary Trademark Liability after Tiffany v. eBay*, 24 BERKELEY TECH. L.J. 491, at 494 (2009).
[357] 18 U.S.C.§2510(12): "electronic communication" means any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce.
[358] Mark A. Lemley, *Rationalizing Internet Safe Harbors*, 6 J. on TELECOMM. & HIGH TECH. L. 101 at 105, (2007).
[359] 15 U.S.C.§1114(2)(B).
[360] Lemley, *supra* note 358, at 106.
[361] Lemley, *supra* note 358, at 106.
[362] *Hendrickson v. eBay*, 165 F. Supp. 2d 1082 (2001).
[363] *Tiffany (NJ) Inc. v. eBay Inc.*, 600 F.3d 93 (2d Cir. 2010) [hereinafter *eBay II*].

buy. Plaintiff is the copyright owner of the documentary "Mason." In 2000, plaintiff detected pirated copies of "Mason" in DVD format were available on eBay posted by its sellers. It sought copyright and trademark injunctions against eBay and its sellers, and also sought to hold eBay accountable for secondary liability for copyright and trademark infringements.

With regards to plaintiff's trademark claim against eBay, the court held that eBay would be an "innocent infringer" within the meaning of Section 32(2) of the Lanham Act because the undisputed facts showed that eBay had no knowledge of a potential trade dress violation before the plaintiff filed suit.[364] Moreover, although eBay removed the allegedly false and misleading advertisements identified by plaintiff, "plaintiff seeks an injunction enjoining any and all false and/or misleading advertisements that may be posted on eBay's website by users in the future."[365] Furthermore, the court rejected the plaintiff's claim because "such an injunction would effectively require eBay to monitor the millions of new advertisements posted on its website each day and determine, on its own, which of those advertisements infringe Plaintiff's Lanham Act rights."[366]

As a result, the court ruled that "eBay has no affirmative duty to monitor its own website for potential trade dress violation and plaintiff had failed to put eBay on notice that particular advertisements violated his Lanham Act rights before filing suit."[367] In conclusion, despite the fundamental difference between copyright and trademark, the court adopted a similar rationale from secondary copyright infringement theory of ISPs to secondary trademark infringement theory of ISPs such as: (1) ISPs have no affirmative duty to monitor their own websites for potential trademark violations; (2) Trademark owners have to notify ISPs on particular trademark infringement activities in order to obtain potential injunctions under Lanham Act; and (3) ISPs have to be "innocent infringers" under Section 32(2) of the Lanham

[364] *Hendrickson*, at 1095.
[365] *Id*.
[366] *Id*.
[367] *Id*.

Act in order to gain exemption from trademark safe harbor.

b. *Tiffany (NJ) Inc. v. eBay Inc.*

Although Section 32(2) of the Lanham Act provides safe harbor provision for ISPs, the court tends to adopt secondary trademark infringement theory developed by case law to solve the online trademark issues. In *eBay* case, the plaintiff Tiffany (NJ) Inc. ("Tiffany") became aware that counterfeit Tiffany merchandise was being sold on defendant eBay's website. To prevent online trademark infringement, eBay set up a "Verified Rights Owner Program" ("VeRO"), a N&T system that is similar to the DMCA, allowing IP owners to report to eBay any listing offering potentially infringing items by a "Notice of Claimed Infringement" ("NOCI") form, so that eBay could remove such reported listings.[368] Because eBay was involved in trademark infringement by its sellers, the issue focused on whether eBay was liable for secondary trademark infringement. Before discussing this issue, the court cited a test in *Inwood Inc. v. Ives Inc.*,[369] which is known as the applicable (*Inwood)* standard.

i. *Inwood* standard

Before the digital age, the U.S. Supreme Court concluded a test for contributory trademark infringement in *Inwood*:

> If a manufacturer or distributor intentionally induces another to infringe a trademark, or if it continues to supply its product to one whom it knows or has reason to know is engaging in trademark infringement, the manufacturer or distributor is contributorially responsible for any harm done as a result of the deceit.[370]

However, the first issue is whether the *Inwood* test can be extended to contributory trademark infringement of ISPs in the digital age. The district court concluded that the *Inwood* test applied to ISPs that exercise sufficient control over the means of the infringing conduct.[371] The Second

[368] *eBay II*, at 99.
[369] *Inwood Laboratories, Inc. v. Ives Laboratories, Inc.*, 456 U.S. 844 (1982).
[370] *Inwood*, 456 U.S. 844, at 854.
[371] *Tiffany (NJ) Inc. v. eBay Inc.*, 576 F.Supp.2d, at 505-506 (2008) [hereinafter *eBay I*].

Circuit agreed and analyzed the second issue: whether eBay is liable under the *Inwood* test. Tiffany did not argue the inducement prong of the *Inwood* test, which is whether eBay intentionally induces another to infringe Tiffany's trademark. As a result, the issue focused on the knowledge prong of the *Inwood* test, which is whether "eBay continued to supply its services to the sellers of counterfeit Tiffany goods while knowing or having reason to know that such sellers were infringing Tiffany's mark."[372]

The district court concluded that "while eBay clearly possessed general knowledge as to counterfeiting on its website, such generalized knowledge is insufficient under the *Inwood* test to impose upon eBay an affirmative duty to remedy the problem."[373] The Second Circuit agreed and further elaborated that "[f]or contributory trademark infringement liability to lie, a service provider must have more than a general knowledge or reason to know that its service is being used to sell counterfeit goods. Some contemporary knowledge of which particular listings are infringing or will infringe in the future is necessary."[374] Therefore, merely general knowledge that ISPs' services is being used as trademark infringement is not enough to impose contributory trademark liability on ISPs. To prove that ISPs supply their services to individuals who know or have reason to know are infringing trademarks, constructive knowledge of particular and identifiable infringements, such as NOCIs, is necessary. Because eBay removed the infringement listing and suspended repeat offenders based on NOCIs, the Second Circuit held that eBay was not contributorily liable for trademark infringement.[375]

[372] *eBay II*, at 106.
[373] *eBay I*, at 508.
[374] *eBay II*, at 106.
[375] *Id.*, at 109.

ii. Relationship with secondary copyright infringement

(1). *Sony*[376] case

In addition, the Second Circuit compared secondary trademark infringement in *Inwood* and secondary copyright infringement in *Sony*, and applied the rationale from secondary copyright infringement theory to solve the secondary trademark infringement issue in *eBay*. It is not rare that courts in the U.S. borrow a doctrine from one IP regime to solve issues in another IP regime.[377] In *Sony*, the U.S. Supreme Court borrowed a staple article of commerce doctrine from the U.S. Patent Law[378] to solve a secondary copyright infringement issue.[379] In *eBay II*, the Second Circuit discussed the U.S. Supreme Court's rationale in *Sony*, and applied *Sony*'s interpretation of *Inwood* on eBay.[380] As a result, the Second Circuit concluded a knowledge requirement that is similar to contributory copyright infringement of ISPs.[381]

(2). *YouTube* case

Coincidentally, in 2010, the Second Circuit also concluded a knowledge requirement on contributory copyright infringement of ISPs in *YouTube*. Notably, the rationale of the knowledge requirement on contributory trademark infringement of ISPs in *eBay*, which is the knowledge prong of the *Inwood* test, is substantially similar to the rationale of the knowledge requirement on contributory copyright infringement of ISPs in *YouTube*. In *YouTube*, the Second Circuit also concluded that mere general awareness about copyright infringements on ISPs' services was not enough. Knowledge of specific and identifiable copyright infringements,[382] such as N&T claims under DMCA, is necessary. Therefore, for contributory

[376] *Sony Corp. of Am. v. Universal City Studios Inc.*, 104 S. Ct. 774 (1984).
[377] *See* Chapter III Part I Section 1 Subsection b Paragraph iii-iv.
[378] *See* 35 U.S.C. § 271(c).
[379] *Sony* at 788.
[380] *eBay II*, at 109.
[381] *Id.*, at 108-109.
[382] *YouTube II*, at 31.

trademark infringement of ISPs and contributory copyright infringement of ISPs, the Second Circuit adopted a similar knowledge requirement.

iii. Willful Blindness

The Second Circuit ruled that ISPs were not permitted willful blindness to trademark infringement by their sellers. "To be willfully blind, a person must suspect wrongdoing and deliberately fail to investigate."[383] Because eBay set up VeRO, removed infringement listing and suspended repeat offenders, the Second Circuit held that eBay did not ignore the information it was given about trademark infringements on its website.[384] As a result, because eBay adopted a DMCA-like VeRO system to prevent trademark infringement by their sellers, the Second Circuit also adopted a DMCA-like approach to the secondary trademark infringement issue of ISPs.

iv. Conclusion

In conclusion, although the Lanham Act does not provide a statutory scheme for N&T system, the case law shows a trend that courts adopt a DMCA-like safe harbor doctrine if ISPs set up a N&T system for trademark protection. Because the DMCA require ISPs to establish a N&T system for copyright protection, most ISPs build a trademark N&T system that is similar to the copyright one. Under this circumstance, courts tend to apply secondary trademark liability theory that has similar rationale as secondary copyright liability theory to solve the trademark issues of ISPs. As a result, this trend has led to the development of similar notice and takedown practices in both copyright and trademark regimes, though without a detailed statutory footing.[385]

---

[383] *Hard Rock Cafe Licensing Corp. v. Concession Services, Inc.*, 955 F.2d 1143, at 1149 (1992).
[384] *eBay II*, at 110.
[385] GRAEME B. DINWOODIE, SECONDARY LIABILITY OF INTERNET SERVICE PROVIDERS 33 (Graeme B. Dinwoodie ed., Springer 2017).

C. Secondary trademark liability of ISPs in China

This Part presents the development of secondary trademark liability of ISPs in China. Section 1 introduces the statute scheme of secondary trademark liability of ISPs, then it examines the impact of the E-commerce Law and the 2017 Anti-unfair Competition Law to ISPs in China. Section 2 examines several cases of ISPs and compares them to the U.S. cases in Part B. First, Section 2 continues to analyze the influential *Tencent* case in Chapter III, so as to address the online unfair competition approach of ISPs in the trademark regime. Second, Section 2 analyzes the development of unfair competition approach of ISPs in the 2017 Anti-unfair Competition Law. Third, Section 2 concludes the relationship between the Internet Clause and the E-commerce Law.

1. Statute scheme of secondary trademark liability of ISPs in China

Section 1 introduces the development of secondary trademark liability of ISPs from different laws and regulations before the new promulgated Anti-unfair Competition Law of the PRC. First, this section introduces the relevant clauses in the Tort Liability Law. Second, this section presents the relevant clauses in the Trademark Law of the PRC and its regulations. Third, this section examines the impact of the E-commerce Law on the secondary trademark liability of ISPs in China.

a. Tort Liability Law of the PRC

Article 36 of the Tort Liability Law constitutes a legal source for secondary trademark infringement liability of ISPs. As mentioned in Chapter III, China adopted joint-liability theory from the Civil Code of the PRC[386] and applied this theory on the liability of ISPs in Article 36.[387] The first paragraph of Article 36 stipulates that both ISPs and network users are liable

[386] Civ. Code of the PRC, art. 178.
[387] *See* Chapter III Part II Section B Subsection 4.

if they directly infringe others' civil rights.[388] The second paragraph of Article 36 stipulates that ISPs are secondary liable for their users' direct infringement if they fail to finish the N&T requirement.[389] The third paragraph of Article 36 set up a knowledge requirement to prevent ISPs from secondary infringement.[390] Because the civil rights in the Civil Code of the PRC include IP rights,[391] Article 36 provides a general doctrine of safe harbor and N&T in trademark regime. However, in *Taobao*, Shanghai First Intermediate People's Court did not adopt the approach that Article 36 provides a safe harbor for secondary trademark liability of ISPs. This point will be discussed later in Section D below.

b. Trademark Law of the PRC

Because Article 36 of the Tort Law is not designed for trademark liability of ISPs, the Third Amendment of the Trademark Law of the PRC[392] and its relevant regulation provide more detail on the secondary trademark liability of ISPs. Article 57 Item (6) of the Trademark Law stipulates that "[a]ny of the following acts shall be deemed infringement of the exclusive right to use a registered trademark … (6) Providing, intentionally, convenience for activities infringing upon others' exclusive right of trademark use, and facilitating others to commit infringement on the exclusive right of trademark use."[393] In other words, Article 57 Item (6) adopts a secondary trademark infringement theory that is similar to a secondary copyright infringement theory, which prevents anyone who intentionally assists or facilitates others to infringe trademark right.

---

[388] Tort Liability Law, *supra* note 51, 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."
[389] Tort Liability Law, art. 36 para. 2.
[390] Tort Liability Law, art. 36 para. 3.
[391] Civ. Code of the PRC, art. 123: "A civil subject shall be entitled to intellectual property rights in accordance with the law."
[392] Zhong hua ren min gong he guo shang biao fa (中华人民共和国商标法) [Trademark Law of the PRC] (first promulgated by the Standing Comm. Nat'l People's Cong. in Fed. 22, 1993, amended by the Standing Comm. Nat'l People's Cong. in Aug. 30, 2013, effective in May 1, 2014) (China). Translated by Westlaw China (www.westlawchina.cn).
[393] Trademark Law of the PRC, art. 57 item (6).

Moreover, Article 75 of the Implementing Regulations of the Trademark Law of the PRC (hereinafter "Trademark Regulation")[394] supplies Article 57 Item (6) of the Trademark Law that "online product transaction platforms" deemed as subjects to facilitate trademark infringement.[395] Although the "online product transaction platforms" are not defined in Trademark Regulation, online retailer platforms such as Amazon or Taobao are generally be considered as platforms where online product transaction occurs. Therefore, Article 75 of the Trademark Regulation supplies Article 57 Item (6) of the Trademark Law, which applies the secondary trademark liability to ISPs and prevent them from facilitating their users to infringe trademark right.

c. The E-commerce Law

The E-commerce Law was promulgated in 2018 to establish a unified IP protection system of ISPs. Notably, the IP protection system of the E-commerce Law emphasizes on improving the serious online counterfeiting and piracy problems of ISPs in China. For example, the online discounter Pinduoduo, which is the third-largest e-commerce platform after Alibaba Group and JD.com, Inc. in China, has been complained about selling counterfeit goods and replicas of brand products by many consumers and trademark holders.[396] Moreover, the State Administration for Market Regulation were also involved to investigate, and required Pinduoduo to obey the law and protect IP in 2018.[397] Therefore, the new E-commerce law, which went into effective on January 1, 2019, set up an important legal foundation to regulate

---

[394] Zhong hua ren min gong he guo shang biao fa shi shi tiao li (中华人民共和国商标法实施条例) [Implementing Regulations of the Trademark Law of the PRC] (promulgated by the St. Council, Apr. 29, 2014, effective in May 1, 2014) (China). Translated by Westlaw China (www.westlawchina.cn).

[395] Implementing Regulations of the Trademark Law of the PRC, art. 75: "Whoever provides warehousing, transportation, mailing or printing services, concealing venues, business premises, online product transaction platforms, etc. for the purpose of infringing upon the right of others to exclusive use of trademarks shall be deemed as providing convenient conditions under Item (6) of Article 57 of the Trademark Law."

[396] Liang Jun & Bianji, China probes online group discounter Pinduoduo over counterfeit allegation, Xinhua (新华网) (Aug. 2, 2018, 08:29), http://en.people.cn/n3/2018/0802/c90000-9486961.html (last visited Aug. 23, 2018).

[397] Liang Jun & Bianji, Pinduoduo told to fix fake goods issue, China Daily (中国日报网) (Aug. 4, 2018, 11:36), http://en.people.cn/n3/2018/0804/c90000-9487727.html (last visited Aug. 24, 2018).

the trademark issues of ISPs in China.

First, the E-commerce Law was designed to regulate ISPs that provide online e-commerce platform, such as Alibaba. For example, Article 2 of the E-commerce Law excludes Internet content providers from the definition of the "electronic commerce" in order to avoid the potential legal conflict between the E-commerce Law and the Third Amendment of the Copyright Law. Therefore, the E-commerce was designed to regulate ISPs such as online transaction platforms that can easily be involved with online counterfeiting and piracy problems.

Second, Article 5 of the E-commerce Law establishes a comprehensive mechanism of ISPs to regulate different areas of ISPs:

> E-commerce operators shall carry out business activities according to the principles of voluntariness, equality, fairness and integrity, abide by laws and business ethics, participate in market competition fairly, fulfill their obligations in terms of consumer rights protection, environmental protection, intellectual property right protection, as well as network security and personal information protection, undertake responsibilities related to the quality of products and services, and accept the supervision of the government and society.[398]

Article 5 constitutes a blueprint for the mechanism of ISPs and imposed comprehensive duties on ISPs. In IP, it sets the layout of a unified IP protection system of ISPs including anti-unfair competition law, IP laws and IP-related laws. It also provides a legal foundation for Chinese legislation to improve IP protection system of ISPs in other relevant laws and regulations in the future. This section focuses on the trademark realm of ISPs and the anti-unfair competition approach will be discussed in the next section.

Third, Article 9 of the E-commerce Law defines ISPs that provide online business transaction platforms, and defines online individual sellers that use ISPs' services. Paragraph 2 defines "E-commerce platform operators" as ISPs that provides network business premises

[398] E-commerce Law, art. 5.

for their sellers to release information and carry out transactions.[399] Paragraph 3 defines "persons doing online businesses over e-commerce platforms" as sellers that use ISPs' services to provide their own products or services.[400] Notably, the definition of E-commerce platform operators does not include Internet content providers such as Netflix or Spotify because (1) Article 2 of the E-commerce Law excludes them from the definition of "electronic commerce;" and (2) Internet content providers provide their services directly to their subscribers. On one hand, because the new Third Amendment of the Copyright Law will provide a specific copyright protection system to ISPs, the Chinese legislation plans to avoid the legal conflict between the E-commerce Law and the new copyright law. On the other hand, different from e-commerce platform operators that provides service to their sellers, Internet content providers, such as Netflix, directly provides their content products to their consumers. Therefore, the E-commerce Law stipulates the safe harbor provision and N&T provision for e-commerce platform operators and their sellers and not for Internet content providers.

Fourth, Article 41 to 45 of the E-commerce law innovatively establishes an active-preventive model of ISPs. Article 41 provides a general active-preventive principle of ISPs. Paragraph 1 and 2 of Article 42 follows the safe harbor doctrine from Article 36 of the Tort Law and stipulates N&T provisions for all IP regime.[401] Article 43 stipulates a counter-notice procedure that is similar to Section 512(g) of the DMCA.[402] The counter-notice procedure of the DMCA is intended to preserve some balance between the subscribers of the ISP, who might have valid grounds for believing that their conduct is not infringing, and the copyright owners,

[399] E-commerce Law, art. 5 para. 2: "For the purpose of this Law, 'e-commerce platform operators' mean legal persons or unincorporated associations that provide two or more parties in e-commerce transactions with services such as network business premises, deal making, and information release for the aforesaid parties to carry out transactions independently."
[400] E-commerce Law, art. 5 para. 3: "For the purpose of this Law, 'persons doing online businesses over e-commerce platforms' mean e-commerce operators who sell products or provide services through e-commerce platforms."
[401] E-commerce Law, art. 42 para. 1 & 2.
[402] 17 U.S.C. § 512(g).

who send the notifications that ISP is likely to comply in order to maintain immunity.[403] Notably, Article 43 expands the counter-notice procedure to all IP regimes, including trademark. In addition, Paragraph 3 of Article 42 follows Section 512(f) of the DMCA[404] and stipulates that any violators who send false notification shall be liable for the damage.[405] Moreover, Paragraph 3 of Article 42 also develops the false notification rule and stipulates that any violators who send false notification with malicious intent shall be liable for double compensation of the damage.[406] This rule is specifically designed to prevent the abuse of the N&T system, which will be further discussed later in Section D.

In conclusion, the E-commerce Law established a new unified IP protection system of ISPs, which can be applied to most of the trademark issues of ISPs. Moreover, because Article 5 of the E-commerce law builds a comprehensive mechanism of ISPs, some trademark issues of ISPs such as unfair competition disputes can also be solved under anti-unfair competition law. The next section introduces the anti-fair competition approach of ISPs in China.

2. The anti-unfair competition approach in Internet context

The anti-unfair competition approach plays an important role to solve online disputes such as unauthorized third-party program. Before the Third Amendment of Trademark Law was promulgated in 2013, whether ISPs could be liable for secondary trademark liability was unclear. Because seeking remedy under trademark law is risky, ISPs in China sought for alternative remedies instead. As a result, Article 2 of the 1993 Anti-unfair Competition Law (hereinafter "General Clause") has been adopted and developed by people's courts to solve certain online disputes in China. Moreover, in 2017, Chinese legislation amended the anti-

[403] DINWOODIE, *supra* note 385, at 33.
[404] 17 U.S.C. § 512(f).
[405] E-commerce Law, art. 42 para. 3.
[406] E-commerce Law, art. 42 para. 3: "If a notification error causes damage to operators doing online businesses over e-commerce platform, any party concerned shall bear civil liability in accordance with the law. Anyone who sends a false notification with malicious intent, causing operators doing online businesses over e-commerce platform to incur loss, the violator shall be liable for double compensation."

unfair competition law and created a new cause of action for ISPs in Article 12 of the 2017 Anti-unfair Competition Law (hereinafter "Internet Clause.")[407] Furthermore, Article 5 of the E-commerce Law also requires ISPs to comply with the principles in anti-unfair competition law.[408]

As a result, the anti-unfair competition approach of ISPs has been developed by case law and become a requirement of ISPs in the E-commerce Law. This Section examines this approach through two cases and statutes. First, this section continues to analyze *Tencent* from Chapter III in the trademark regime. Second, this section presents the General Clause through *Tencent*. Third, this section demonstrates the development of the General Clause for ISPs through *Shanghai Synacast Media Technology Co., Ltd. v. Shanghai Damo Network Technology Co., Ltd.* (hereinafter "*Damo*").[409] Fourth, this section analyzes the impact of the Internet Clause for ISPs in China.

a. *Beijing Qihoo Tech Ltd. v. Beijing Tencent Tech Ltd.*

As mentioned before in Chapter III, Qihoo released an optimization software, Koukou, on its website and advertised that Koukou could repair potential safety hazards of QQ and optimize QQ such as blocking advertainment function.[410] Although Tencent is the copyright and trademark owners of QQ and claimed that Koukou induced users to modify its QQ software without authorization and damaged QQ's goodwill,[411] it filed a lawsuit under the General Clause instead of trademark infringement.

There were two main reasons why Tencent filed an anti-unfair competition lawsuit

---

[407] 2017 Anti-unfair Competition Law, art. 12.
[408] E-commerce Law, art. 5
[409] Shang hai ju li chuan mei ji shu you xian gong si su shang hai da mo wang luo ke ji you xian gong si qi ta bu zheng dang jing zhen jiu fen shang su an (上海聚力传媒技术有限公司诉上海大摩网络科技有限公司其他不正当竞争纠纷上诉案) [*Shanghai Synacast Media Technology Co., Ltd. v. Shanghai Damo Network Technology Co., Ltd.*], Shanghai IP Ct. (上海知识产权法院) Jul 15, 2016, (2016) Hu No. 73 Min Zhong No. 34 [(2016) 沪 73 民终 34 号] (China) [hereinafter *Damo*].
[410] *Tencent*, *supra* note 146, at 3.
[411] *Id.*

instead of a trademark lawsuit. First, neither the Third Amendment of the Trademark Law of the PRC nor its Trademark Regulation was enacted in 2011. Therefore, whether Qihoo could be liable for secondary trademark liability was unclear at that time. Moreover, it was the QQ users who downloaded, installed and ran Koukou on their devices. If QQ users do not commit trademark infringement by using Koukou, Qihoo is not liable for secondary trademark infringement, which requires the existence of direct trademark infringement under secondary trademark liability theory. Thus, it was almost impossible for Tencent to prove that its QQ users constitute direct trademark infringements by using Koukou. Therefore, proving Qihoo was liable under secondary copyright and trademark infringement theories was difficult at that time.

Nonetheless, the Chinese legislation amend the laws immediately to prevent similar issues from happening. Before the Supreme People's court closed the *Tencent* case in February 2014, the Third Amendment of the Trademark Law of the PRC was promulgated in August 2013. Article 57 Item (6) prevent secondary trademark infringement such as providing convenience for infringing activities and facilitating others to commit infringement.[412] Moreover, three months after the *Tencent* case closed, the State Council published the Trademark Regulation in April 2014. Article 75 of the Trademark Regulation stipulates that whoever provides online product transaction platforms for the purpose of infringement shall be deemed as providing convenient conditions under Item (6) of Article 57 of the Trademark Law. As a result, Qihoo is likely to be held liable for facilitating QQ users to commit secondary trademark infringement under the Third Amendment of the Trademark Law of the PRC.

The second main reason why Tencent filed an anti-unfair competition lawsuit is because the General Clause was a broad principle, and therefore People's court was capable of applying it on new Internet issues at that time. Because the General Clause was substantially applied by people's courts on Internet unfair competition cases, Chinese legislation adopted the legal

[412] Trademark Law of the PRC, art. 57 item(6).

experience from these cases into the Internet Clause of the 2017 Anti-unfair Competition Law. The next subsection addresses how the People's court applies General Clause in *Tencent*.

b. 1993 Anti-unfair Competition Law

The General Clause defines unfair competition and stipulates several general anti-unfair competition principles for business operators[413] to comply:

> A business operator shall, in his market transactions, follow the principles of voluntariness, equality, fairness, honesty and credibility and observe the generally recognized business ethics.
>
> "Unfair competition" mentioned in this Law refers to a business operator's acts violating the provisions of this Law, infringing upon the lawful rights and interests of another business operator and disturbing the socio-economic order.[414]

Because the 1993 Anti-unfair competition Law is an old law, there are several issues when applying the General Clause to cases of ISPs. First, whether the General Clause can be applied to IP infringements is questionable. According to Article 123 of the Civil Code of the PRC, because the lawful rights and interests of a business operator include IP rights,[415] IP infringements can be covered under the definition of unfair competition. Second, because the Internet is undeveloped in 1993, whether the General Clause can be applied to Internet market regime is questionable. In *Tencent*, the Supreme People's Court agreed with the trial court's opinion by upholding that the General Clause can be applied on the Internet market regime.[416] Third, because computer technology is undeveloped in 1993, it is unclear whether a software could constitute unfair-competition under the General Clause.

In *Tencent*, the trial court adopted a three-factor test on determining whether Koukou constitutes unfair-competition: (1) Whether Qihoo violated the principles of honesty and credibility; (2) Whether Qihoo violated the generally recognized business ethics of Internet

---

413 1993 Anti-unfair Competition Law, art. 2 para. 3: "A business operator" mentioned in this Law refers to a legal person or any other economic organization or individual engaged in commodities marketing or profit-making services ("commodities" referred to hereinafter includes such services).

414 1993 Anti-unfair Competition Law, art. 2 para. 1.

415 Civ. Code of the PRC, art. 123: "A civil subject shall be entitled to intellectual property rights in accordance with the law."

416 *Tencent*, at 58.

industry; (3) Whether Qihoo damaged Tencent's lawful rights and interests.[417] The trial court analyzed that because Koukou modified the software services of QQ such as advertisements, the safeness of QQ service and users' experience of QQ were damaged. Therefore, Koukou deviated from the technical and business purposes of a safety software. As a result, the trial court held that Qihoo (1) maliciously damaged the integrity of QQ's software and the goodwill of QQ trademark, and (2) caused economic loss on QQ services such as advertisements, which constituted unfair competition.[418]

The Supreme People's Court agreed with the trial court's opinion by combining the three-factor test into two key issues: (1) whether the act of Qihoo violated the principles of honesty and credibility, and the generally recognized business ethics of Internet industry; (2) whether the act of Qihoo damaged Tencent's lawful rights and interests.[419] Instead of analyzing these two issues separately, the Supreme People's court discussed these two issues as a whole. First, the Supreme People's court recognized that Tencent adopted a business model that provided QQ as a platform for free and profited from value-added service such as advertisement. This business model did not violate the principles of anti-unfair competition law, therefore the lawful rights and interests of Tencent should be protected. Second, Qihoo specifically developed and managed Koukou for QQ software. By facilitating and inducing QQ users to use Koukou, Koukou damaged the integrity and safety of QQ software, which caused profit loss on value-added services of QQ.[420] Therefore, the Supreme People's Court held that (1) Qihoo disturbed Tencent's business activities of QQ, (2) Qihoo damaged the lawful rights and interests of Tencent, and (3) Qihoo violated principles of honesty and generally recognized business ethics.[421]

---

[417] *Tencent*, at 23.
[418] *Id*., at 24-25.
[419] *Id*., at 58.
[420] *Id*., at 59.
[421] *Id*.

In conclusion, on determining whether Qihoo constitutes unfair-competition, the Supreme People's Court adopted a similar rationale of the secondary copyright infringement theory. First, whether Qihoo directly infringed Tencent's lawful rights and interests. Second, whether Qihoo facilitated and induced QQ users to use Koukou. This rationale was also adopted and developed by the Shanghai IP Court in *Damo*, which will be examined in the next subsection.

c. *Shanghai Synacast Media Technology Co., Ltd. v. Shanghai Damo Network Technology Co., Ltd.*

Because *Tencent* was an influential case, ISPs in China tends to follow this anti-unfair competition approach to solve the issue of unauthorized third-party software. The Shanghai IP Court adopted and developed the anti-unfair competition approach from *Tencent* and applied it in *Damo*. In *Damo*, defendant-appellate Shanghai Damo Network Technology (hereinafter "Damo") developed and managed an advertisement filtering software, "ADSafe," in 2014. ADSafe filters advertisements from software or webpage by blocking the operation of the advertisement code.[422] Plaintiff-appellee Shanghai Synacast Media Technology (hereinafter "Synacast") operated a website "www.pptv.com" (hereinafter "PPTV") that provided VOD services to the public. To watch a video for free, a PPTV user has to watch an advertisement first. Otherwise, a PPTV user has to subscribe in order to watch video without advertisement. If a PPTV user installed ADSafe software and activated the advertisement filter, ADSafe would stop the advertisement request and allow the playing request of the video.[423] In other words, the advertisement filter of ADSafe allowed the PPTV users who were unwilling to subscribe to skip the advertisement before watching the video. Because ADSafe allowed PPTV users to watch video without advertisements and subscriptions, Synacast filed an unfair competition

[422] *Damo*, Shanghai IP Ct., *supra* note 409, at 4. *See also* SHANGHAI IP COURT, *supra* note 311, at 567.
[423] *Damo*, at 5. *See also* SHANGHAI IP COURT, *supra* note 311, at 568.

lawsuit against Damo.

Both the trial court and the Shanghai IP court followed the anti-unfair competition approach from *Tencent* and focused the issue on whether Damo developed and managed ADSafe software constituted unfair competition. The Shanghai IP court concluded that "the key is to determine whether advertisement filter of ADSafe has violated the principle of good faith and generally recognized business ethics and damaged legitimate rights and interests of Synacast."[424] Compared to the facts in *Tencent*, the main difference between *Damo* and *Tencent* is that Damo did not specifically design or advertise ADSafe for PPTV. Neither the advertisement filter of ADSafe nor the slogan of ADSafe, "no waiting before watching videos," mentioned PPTV. While in *Tencent*, not only did Qihoo develop Koukou for QQ software, but also advertised Koukou by including the "QQ" trademark. The Supreme People's Court held that because Koukou deeply intervened the normal operations of QQ software, Qihoo's act damaged lawful rights and interests of QQ and constituted unfair competition.[425] Based on this difference, Damo argued that it merely provided ADSafe to users as a neutral technical software, which did not constitute unfair-competition.[426]

Shanghai IP court rejected Damo's argument and demonstrated that Damo was fully aware that the advertisement filter of ADSafe would directly damage commercial interests of Synacast. However, Damo still promoted ADSafe to the public including PPTV users.[427] Even though ADSafe was not specifically designed for PPTV, Damo facilitated and induced PPTV users who were unwilling to subscribe to breach the agreement between PPTV and its users. Because the advertisement filter of ADSafe allowed PPTV users to watch video without advertisements and subscriptions, Shanghai IP Court held that the act of Damo damaged lawful rights and interests of Synacast for its own competitive advantages and therefore constitute

[424] *Damo*, at 11. *See also* SHANGHAI IP COURT, *supra* note 311, at 574.
[425] *Tencent*, at 57.
[426] *Damo*, at 10.
[427] *Id.*, at 11.

unfair competition.[428]

In conclusion, unlike *Tencent*, even though Damo did not specifically develop ADSafe for Synacast, Damo's act constituted unfair competition because ADSafe facilitated PPTV users to watch videos without advertisements. This rationale was adopted by the Chinese legislation and developed in the Internet Clause of the 2017 Anti-unfair Competition Law.

d. 2017 Anti-unfair Competition Law

Based on the experience of case law, the Chinese legislation decided to enact a clause that regulates unfair competition issues of ISPs in the new 2017 Anti-unfair Competition Law, so as to regulate the online unfair competition cases. The Internet Clause clarifies that ISPs shall comply with the principles of Anti-unfair Competition Law[429] by stipulating:

> A business operator shall not use technical means to carry out any of the following activities that obstruct or disrupt the normal operations of the online products or services lawfully provided by other business operators by way of affecting users' choices or otherwise:
> (1) Where the business operator, without consent from other business operators, inserts links in the online products or services lawfully provided by the latter, or forces the redirection of targets;
> (2) Where the business operator misleads or compels users to modify, close or uninstall the online products or services that are lawfully provided by other business operators, or deceives users into modifying, closing or uninstalling such products or services;
> (3) Where the business operator maliciously causes incompatibility with the online products or services that are lawfully provided by other business operators; or
> (4) Where the business operator commits any other acts that obstruct or disrupt the normal operations of the online products or services lawfully provided by other business operators.[430]

Item (1) to (3) of the Internet Clause adopt the rationale from the recent unfair competition cases of ISPs such as *Tencent* and *Damo*, which list three causes of action to prevent unfair competition activities via Internet. Item (4) of the Internet Clause is a miscellaneous rule that prevents any other online unfair competition activities that may occur in the future.

---

[428] *Damo*, at 10. *See also* SHANGHAI IP COURT, *supra* note 311, at 573.
[429] 2017 Anti-unfair Competition Law, art. 12 para. 1: "A business operator shall comply with this Law when engaging in production and business activities by using the Internet."
[430] 2017 Anti-unfair Competition Law, art. 12 para. 2.

Not only does the Internet Clause directly prevent unfair competition disputes of ISPs, but it also indirectly prevents online IP infringements. For example, although the Supreme People's Court did not explicitly state that Koukou infringed the copyright of QQ software and the "QQ" trademark in *Tencent*, it concluded that Qihoo's act maliciously modified the QQ software[431] and damaged the goodwill of the QQ trademark.[432] Because Item (2) of the Internet Clause clearly prevents any "technical means" to mislead users to modify other ISPs' online services or products,[433] it is possibly for IP owners to seek remedy under the Internet Clause. Therefore, the rationale embodied in the *Tencent* has been merged into the Internet Clause. However, the term "technical means" is not defined in the 2017 Anti-unfair Competition Law. According to Item (4) of the Internet Clause, technical means should be broad enough to cover any technical measures that are now known or later developed. As a result, the Internet Clause provides an alternative solution for IP owners to solve online disputes such as unauthorized third-party programs.

e. Relationship between the Internet Clause and the E-commerce Law

In conclusion, the Internet Clause is one of the components in the unified IP protection system of ISPs established by the E-commerce Law. Not only does Article 5 of the E-commerce Law impose ISPs to protect IP, but it also require ISPs to (1) carry out business activities according to the principles of voluntariness, equality, fairness and integrity, (2) abide by laws and business ethics and (3) participate in market competition fairly.[434] In other words, Article 5 of the E-commerce Law requires ISPs to abide by the principles in Anti-unfair Competition Law, and the Internet Clause stipulates particular anti-unfair competition requirements for ISPs. As a result, the anti-unfair competition approach becomes an important supplement for IP

[431] *Tencent*, at 57.
[432] *Id.*, at 63.
[433] 2017 Anti-unfair Competition Law, art. 12 para. 2 item (2).
[434] E-commerce Law, art. 5.

protection system of ISPs in China.

D. Case

This section presents a secondary trademark case of ISPs to show how the people's court solve online trademark infringement disputes in China. After analyzing *E. LAND Ltd. v. Taobao Network Ltd.* (hereinafter "*Taobao*"),[435] this section makes a comparison with *eBay* so as to conclude the similarity and differences of the secondary trademark liability of ISPs between China and the U.S.

1. *E.LAND Ltd. (Shanghai) v. Zhejiang Taobao Network Ltd.*

a. Background

Defendant-appellate Zhejiang Taobao Network Ltd. (hereinafter "Taobao") and its parent company, Alibaba Group, operates one of the biggest online transaction platforms in China, "www.taobao.com," where sellers can list goods for sale. In the first half of 2009, Taobao had almost 0.145 billion users and its business transaction volume was up to RMB 80.6 billion (approximately USD 11.9 billion).[436] Plaintiff-appellee E.LAND Ltd. (hereinafter "E.LAND") was the trademark owner of clothing marks "E.LAND" and "TEENIEWIENEE." These two marks were rewarded 2009 annual famous brand in Shanghai.[437] Co-defendant Du Guofa (hereinafter "Du") was an individual seller of Taobao. According to the transaction records on Taobao, from December 2009 to February 2010, Du sold around twenty counterfeit TEENIEWIENEE clothes through his Taobao account.[438] Since September 2009, plaintiff

[435] Yi nian (shang hai) shi zhuang mao yi you xian gong si su zhe jiang tao bao wang luo you xian gong si, du guo fa qing hai shang biao quan jiu fen [衣念（上海）时装贸易有限公司诉浙江淘宝网络有限公司、杜国发侵害商标权纠纷] [E. LAND Ltd. (Shanghai) v. Zhejiang Taobao Network Ltd.], [Shanghai First Interm. People's Ct. (上海市第一中级人民法院)] [(2011) Hu Yi Zhong Min Wu (Zhi) Zhong Zi No. 40 (沪一中民五(知)终字第 40 号)] (China) [hereinafter *Taobao*].
[436] *Taobao*, Shanghai First Interm. People's Ct., *supra* note 435, at 2.
[437] *Id.*
[438] *Id.*, at 1.

detected massive amount of counterfeit clothes of its trademarks on Taobao. For Du's infringing activities, the plaintiff sent notifications to Taobao seven times and request Taobao to stop the infringing activities. Although Taobao blocked the potentially infringing listings each time, it did not permanently block Du's account and allowed Du to continue his business on Taobao. Therefore, the plaintiff filed a trademark infringement lawsuit against direct infringer Du and joint-infringer Taobao, claiming that even though Taobao was fully aware that Du was infringing plaintiff's trademark, it did not take further measures to stop the infringing activities. Thus, Taobao was liable for contributary trademark infringement because it intentionally provided convenience to Du and facilitated Du's infringing activities.[439]

b. Trial court's decision

At trial, Taobao counterclaimed that the plaintiff abused its N&T policy. Taobao established a N&T policy where IP owners could send notifications of potentially infringing listings to Taobao. After manual review, Taobao would remove the notified listing. The sellers of Taobao could counter the notification by sending a statement to Taobao, including prima facie evidence showing that there is no infringement. Taobao would forward the statement to IP owners in light of its N&T policy. This N&T policy was later developed by its parent company Alibaba Group, and established the Alibaba Intellectual Property Protection (hereinafter "AIPP") platform where IP owners can file complaints in the form of take-down requests on listed products or product descriptions that allegedly infringe their IPRs.[440]

From September to November 2009, the notifications reported from the plaintiff included 105643 of potentially infringing listed items, but approximately 20% of the plaintiff's notifications were false notifications. For the seven notifications against Du, four notifications were irrelevant to the plaintiff's trademarks, and none of them included any evidence to prove

[439] *Taobao*, at 2.
[440] Alibaba Group, *IPP Platform Principle & Policy*, Available at https://ipp.alibabagroup.com/policy/en.htm (last visited Oct. 19, 2018).

that Du was selling counterfeit clothes. Each time Taobao received notifications from the plaintiff, it removed the potentially infringing listings immediately, and Du never sent counter notifications to Taobao. Because Taobao adopted reasonable measures to protect the plaintiff's trademark, therefore, it should not be liable for contributary trademark infringement.[441]

The trial court concluded that there were three issues: (1) whether Du's act infringed the plaintiff's trademarks; (2) whether Taobao knew its user's infringing activity and whether Taobao took necessary measures to prevent infringement; and (3) whether Taobao was liable for contributary trademark infringement.[442] For the first issue, the trial court held that Du directly infringed on the plaintiff's trademarks.[443] For the second issue, the trial court recognized that even though the ISPs removed the potentially infringing listings after receiving the notifications, the ISPs should act further and adopt necessary measures to prevent repeat infringements.[444] Depending on the category of ISPs, feasibility of technology, infringement and cost, the necessary measures might be different. For ISPs that provide online transaction platforms, necessary measures should include warnings, suspending sellers and even permanently blocking the account. Because Du was reported seven times by the plaintiff, Taobao should have known that Du used its online transaction platform to sell infringing goods. However, besides removing the infringing listings, Taobao did not adopt any further necessary measures to stop the infringing activities.[445] For the third issue, the trial court held that Taobao had subjective fault to keep providing its service to Du, and intentionally provided convenience to Du to sell infringing counterfeit goods. Therefore, Taobao was liable for contributary trademark infringement.[446]

---

441 *Taobao*, *supra* note 435, at 3.
442 *Id.*, at 3.
443 *Id*.
444 *Id.*, at 4.
445 *Id*.
446 *Id*.

c. Shanghai First Intermediate People's Court's decision

Shanghai First Intermediate People's Court affirmed the trial court's decision and further construed the knowledge requirement on whether ISPs should be liable for contributary trademark liability. Because ISPs are not capable of predicting or preventing their users' infringing activities, therefore, ISPs should not be liable for their users' direct infringing activities. However, if ISPs know or should have known that their users commit infringements, but still provide service to infringers and do not adopt appropriate measures to prevent infringements, ISPs shall be jointly liable for infringements.[447]

For ISPs, on determining whether their users involve infringements, not only shall the ISPs examine evidence from the notifications, but shall also examine the users' counter notifications. Generally, if a seller's legitimate listings are removed by Taobao, the seller would not ignore it. On the contrary, the seller would actively react and send counter notification unless the listed items truly infringe trademark. In this case, even though Du's listings of goods were removed multiple times, Du never react or sent counter notifications to Taobao. Therefore, Taobao was fully aware that Du was selling infringing counterfeit products.[448]

Even though Taobao argued that some of the plaintiff's notifications were false notifications, the court believed that a notification was valid as long as it included information of the potential infringing activities and the proof of trademark owner's exclusive rights. For the seller who involves infringement, one valid notification is sufficient to indicate that the ISPs know the existence of infringing facts, and the ISPs rationally recognize whether the seller commit infringements. Therefore, the court held that even though Taobao knew that Du directly infringed a trademark via its service, it just passively removed the infringing listing based on the notifications. However, it was deficient to stop the infringing activities of Du. Because

[447] *Taobao*, at 6.
[448] *Id*.

Taobao did not adopt necessary measures to prevent the infringing activities, it had subjective fault that objectively facilitated Du's infringing activities. As a result, Taobao was liable for contributary trademark infringement and bore joint compensation liability for Du's direct trademark infringement.[449]

d. Secondary trademark liability theory of ISPs from *Taobao* and *eBay*

Compared to *eBay*, the contributary trademark infringement theory of ISPs from Taobao is similar to the theory from *eBay*. First, both courts from China and the U.S. point out that ISPs do not have affirmative duty to inspect their service. Second, both courts developed their secondary trademark liability theory of ISPs from their tort laws. In *Taobao*, the Shanghai First Intermediate People's Court developed the safe harbor doctrine and Red Flag knowledge provision from Article 36 of the Tort Liability Law, and applied them to the online trademark issues. In *eBay*, the Second Circuit developed the contributory trademark theory from *Inwood* and applied the Inwood test to trademark issues of ISPs. Third, both courts considered the knowledge requirement of ISPs as the key to determine whether ISPs shall be liable for secondary trademark liability.

Both courts emphasize that merely general knowledge about the potential infringement on ISPs' service is insufficient to impose contributory trademark liability on ISPs. To prove that ISPs know or should have known their users' infringing activities, IP owners have to send eligible notifications with constructive knowledge of particular and identifiable infringement. Therefore, once ISPs know a particular infringement, merely removing the infringing listing is not enough. The ISPs have to adopt affirmative measures to stop and prevent the repeat infringement.

Even though the Shanghai First Intermediate People's Court ruled against the ISPs in

[449] *Taobao*, at 6.

Taobao while the Second Circuit upheld ISPs in *eBay*, both courts adopted the same rule of thumb on the contributory trademark infringement issues of ISPs. Because both *Taobao* and *eBay* established a DMCA-like N&T system for IP owners, the main difference between these two cases was that eBay removed infringing listing and suspended repeat infringers based on notifications, while Taobao merely removed infringing listing even if it was notified infringements by the plaintiff for multiple times. In *Taobao*, the court pointed out that Taobao should have strictly followed its N&T policy to prevent infringements, such as blocking the repeat infringer's account.[450] Thus, if Taobao blocks the infringer's account, it is possible that the Shanghai First Intermediate People's Court may follow *eBay* and hold that Taobao is not liable for contributory trademark infringement.

e. Conclusion

In conclusion, before the E-commerce law establishes a unified IP protection system of ISPs, the secondary trademark liability theories of ISPs are similar between China and the U.S. Although there is no statutory requirement for ISPs to adopt a DMCA-like N&T system for trademark protection in China, the ISPs set up a trademark N&T system that is similar to the copyright one. For the secondary trademark liability issues of ISPs, people's courts tend to apply the safe harbor doctrine and the Red Flag knowledge provision from Article 36 of the Tort Liability Law to solve trademark infringement issues.

However, because Article 36 of the Tort Liability Law followed the passive-reactive approach of ISPs, the court recognized that removing the infringing listings based on the notifications passively is deficient for ISPs to stop the online infringements.[451] As a result, Chinese legislation adopted an active-preventive approach of ISPs in the new E-commerce Law.

[450] *Taobao*, at 3.
[451] *Taobao*, at 6.

E. The impact of the E-commerce Law for ISPs in China

Part E analyzes the impact of the new E-commerce Law before and after its promulgation in China. Section 1 examines the active-preventive approach of Alibaba to prevent the IP infringements through its platform. Section 2 construes the active-preventive model of ISPs of the E-commerce Law and how it impacts the ISPs in China.

1. The active-preventive approach of Alibaba

a. Background

ISPs can voluntarily contribute to efforts to restrain trademark infringements on their platforms. For example, after *Taobao*, Alibaba recognized the importance of preventing IP infringement through its platforms and adopted multiple measures to engage in IP protection. Notably, during the 2017 NPC and the National Committee of the Chinese People's Political Consultative Conference (CPPCC), Alibaba Group Founder and Executive Chairman, Jack Ma, appealed to Chinese legislators to strengthen laws and toughen penalties for counterfeiting. Moreover, Jack Ma also urged the representatives of the NPC and CPPCC to crack down counterfeiting.[452] As a result, not only did Alibaba adopt an active-preventive approach to IP protection on its platform, but also promoted Chinese legislation to adopt an active-preventive approach in the E-commerce Law.

b. The active-preventive approach of Alibaba

Before the E-commerce Law, Alibaba adopted multiple measures to actively prevent IP infringement through its platforms. According to the Alibaba Group 2017 Intellectual Property Rights Protection Annual Report (hereinafter "2017 IP Report"), the active-preventive approach of Alibaba can be divided into two categories. First, Alibaba enhanced and developed

[452] Alibaba Group, *Alibaba Group 2017 Intellectual Property Rights Protection Annual Report*, Available at http://azcms31.alizila.com/wp-content/uploads/2018/05/Alibaba-Group-PG-Annual-Report-2017-FINAL_sm_final.pdf (last visited Oct. 20, 2018) [hereinafter 2017 IP Report].

multiple technical measures to actively detect and prevent the potential infringement. Second, Alibaba actively cooperated with IP holders, Law Enforcements and Internet users to detect potential infringement and crack down counterfeiting.

i. Technical measures of Alibaba

First, Alibaba improved the N&T system on its AIPP platform and introduced the Express Intellectual Property Protection (EIPP) service in June 2017. The EIPP is a significant technical measure that increases the speed of IPR holders' takedown requests by enhancing algorithms and data modeling.[453] According to the 2017 IP Report, 95% of legitimate IPR takedown requests submitted through the EIPP were processed within 24 hours.[454]

Second, Alibaba applied multiple proactive monitoring technical measures to detect potentially problematic listings. Although a traditional passive-reactive approach does not require ISPs to actively monitor its service,[455] Alibaba adopted an active-preventive approach on IP protection by using proactive monitoring technical measures such as Real-Time Interception System, Product Information Library, or Image and Semantic Recognition Algorithms.[456] For example, the Real-Time Interception System "[o]perates in real-time to conduct risk assessment scans within microseconds of a product's listing or editing to identify and intercept potentially problematic listings."[457]

Third, when Alibaba's proactive monitoring technical measures detect potentially problematic listings, its Data Sampling Model determines whether it shall launch the Test-Buy Program for further manual review.[458] Through the Test-Buy Program, Alibaba purchased potentially problematic products from their sellers to further verification. According to the

[453] 2017 IP Report, *supra* note 452, at 4.
[454] 2017 IP Report, at 4.
[455] See e.g. 17 U.S.C. § 512(m)(1). See also 2012 Provision, art. 8 para. 2.
[456] 2017 IP Report, at 10-11.
[457] 2017 IP Report, at 11.
[458] 2017 IP Report, at 11.

2017 IP Report, Alibaba spent approximately RMB 100 million (approximately USD 14.76 million) on its Test-Buy Program to verify whether the potentially problematic products constitute counterfeit.[459] Alibaba imposed penalties against the sellers immediately when the involving products confirmed to be counterfeit, and even filed lawsuits against repeat infringers. As a result, Alibaba establishes an active-preventive mechanism through its proactive monitoring and Test-Buy Program. By applying proactive monitoring technical measures to intercept and detect potentially problematic listings, Alibaba shifted from a passive-reactive approach to an active-preventive approach on IP protection.

ii. Cooperation

(1). Cooperation with IP holders

In January 2017, Alibaba cooperated with 30 other leading domestic and international trademark owners and founded the Alibaba Anti-Counterfeiting Alliance (AACA), a first of its kind anti-counterfeiting alliance. On one hand, AACA provides IP holders with an established channel to influence Alibaba IPR policies and practices. On the other hand, AACA combines IP holders' knowledge with Alibaba's insights to protect IPR more effectively.[460] Therefore, by actively cooperating with IP holders, Alibaba established a platform where IP holders can engage with ISPs regarding IP protection.

(2). Cooperation with Internet users

In 2012, Alibaba founded the Alibaba Public Jury program where Internet users can participant as juries to determine whether the potentially problematic listings constitute infringements.[461] For example, when Alibaba's proactive monitoring technical measures

[459] 2017 IP Report, at 6.
[460] 2017 IP Report, at 22.
[461] ALIBABA PUBLIC JURY, HTTPS://PAN.TAOBAO.COM (LAST VISITED DEC. 25, 2018).

detect a potentially problematic product, the product's information will be sent to at least 500 public juries to verify. If a majority of the juries determine that the product constitute infringement, Alibaba would take further steps to prevent the infringement.

From 2012, more than 17.2 million Internet users participated in the Alibaba Public Jury program, and more than 160 million cases were verified under the program.[462] The Alibaba Public Jury program provides an alternative solution for ISPs to verify potentially infringing activities, which benefits both Internet users and IP holders. Through the Alibaba Public Jury program, Internet users can engage into the IP protection process of ISPs, which helps the IP holders to prevent the online IP infringement.

(3). Cooperation with Law Enforcements

Other than online IP protection, Alibaba also established Alibaba's Anti-Counterfeiting Special Task Force to help combat offline counterfeit production and sales with Law Enforcement.[463] For example, in November 2017, the Chinese Ministry of Public Security announced that the Sino-U.S. police successfully cracked an extremely large number of cross-border criminal IPR infringement cases. The criminal enterprise had accumulated sales amounting to RMB 100 million (approximately USD 14.76 million). In 2015, trademark owners reported a Taobao seller and sought assistance from Alibaba. Through investigation, the Alibaba Anti-Counterfeiting Special Task Force determined that the criminal enterprise had initially tried to sell counterfeit goods through a Taobao store. After the online store was terminated by Alibaba, the criminal enterprise established an independent website to sell counterfeit goods to the U.S. and Europe. With the cooperation of Alibaba, the police discovered the domain name registrar was a Guangdong company, but the website server was located in the U.S. Chinese law enforcements launched a raid at production, logistics,

[462] ALIBABA PUBLIC JURY, HTTPS://PAN.TAOBAO.COM (LAST VISITED DEC. 25, 2018).
[463] 2017 IP Report, at 11.

packaging and warehousing facilities of the criminal enterprise and the U.S. law enforcement agencies simultaneously conducted investigations on their domestic websites.[464] As a result, Alibaba cooperated with both domestic and foreign law enforcements to crack down both online and offline IP infringements.

iii. Conclusion

As a pioneer of Chinese ISPs, not only did Alibaba innovatively develop technical measures to proactively monitor its platforms, but also actively cooperated with stakeholders to prevent IP infringement. With a great achievement on IP protection in 2017,[465] the Chinese legislation also adopted an active-preventive approach of ISPs and enacted the E-commerce Law in 2018, which will be discussed below.

2. The active-preventive approach of the E-commerce Law

This section analyzes the impact of the new E-commerce Law for ISPs in China. By examining the advantages and drawbacks of the unified IP protection system of ISPs, this section proposes several suggestions for Chinese legislation on how to improve the system of ISPs established by the E-commerce Law.

a. Advantages of a unified IP protection system of ISPs

The E-commerce law established a unified IP protection system for ISPs, which provides greater certainty in the area of trademark infringement in the Internet. For example, several issues in *Taobao* can be clarified under the new E-commerce Law. First, the E-commerce established a unified N&T system for IP holders to notify ISPs, and for sellers of ISPs to counter notifications. In *Taobao*, Taobao argued that some of the plaintiff's notifications were false notifications because none of them included any evidence to prove that Du was

[464] 2017 IP Report, at 14-15.
[465] *See e.g.* 2017 IP Report, at 4-6.

selling counterfeit clothes. The E-commerce Law requires both notification and counter notification to include prima facie evidence. Article 42 of the E-commerce Law stipulates that "[t]he notification shall include prima facie evidence concerning the infringement,"[466] and Article 43 of the E-commerce Law stipulates that "[t]he statement shall include prima facie evidence showing that there is no infringement."[467] Following these requirements, ISPs such as Alibaba Group established the AIPP platform where IP holders can send notification on listed products or product descriptions that allegedly infringe their IPRs.[468]

Second, because the ISPs are not official institution to examine IP, Article 43 of the E-commerce Law imposes an obligation to ISPs, which requires them to forward the counter notifications to the IP holders and notify their legal rights to file complaints to administrative departments or lawsuits to people's courts. Moreover, Article 43 also provides a fifteen-day grace period for IP holders to file complaints or lawsuits after they receive the counter notifications, otherwise the ISP shall "terminate the measures taken if it does not receive a notification showing that the right holder has filed a complaint or lawsuit."[469] However, the E-commerce Law does not provide further detail on how the people's court shall solve the online trademark disputes of ISPs.

Nonetheless, the Internet Court provides an easy and effective way to solve the online trademark disputes of ISPs. For example, the Hangzhou Internet Court has jurisdiction to hear cases arising from "online shopping or online services."[470] Moreover, because it also

---

[466] E-commerce Law, art. 42 para. 1.
[467] E-commerce Law, art. 43 para. 1.
[468] Alibaba Group, *IPP Platform Principle & Policy*, *supra* note 440.
[469] E-commerce Law, art. 43 para. 2: "Upon receipt of the abovementioned statement, the e-commerce platform operator shall forward it to the intellectual property right holder who sent the infringement notification, and inform the latter that a complaint may be filed with the relevant competent department or a lawsuit filed with the people's court. The e-commerce platform operator shall, within 15 days after forwarding the statement to the intellectual property right holder, terminate the measures taken if it does not receive a notification showing that the right holder has filed a complaint or lawsuit."
[470] Hangzhou Internet Court (杭州互联网法院), Hangzhou Internet Court's Guidelines Regarding the Litigation and Jurisdiction of the Internet-involved Cases (杭州互联网法院案件管辖指引), art. 1. Available at https://www.netcourt.gov.cn/portal/main/domain/lassen.htm?lang=En#lassen/litigationDocuments (last visited Nov. 25, 2018).

established an electronic evidence platform to "store, access, exchange or examine the electronic evidence,"[471] IP holders can easily file lawsuits and submit electronic evidence online. As a result, ISPs can notify the IP holders to file lawsuits against potential infringers through the online litigation platform of the Internet court, and transfer the relevant evidence through the electronic evidence platform to the Internet Court.

Third, Paragraph 3 Article 42 of the E-commerce Law provides a false notification rule to prevent the abuse of the N&T system. The sellers of ISPs can seek remedy under Article 42 for the damage of the false notification.[472] Moreover, for anyone who send false notification to ISPs with malicious intent and cause damage, Article 42 stipulates that the violator shall compensate for double of the damage.[473] For example, a seller of ISP sends a notification against its business competitor before the Black Friday sale, claiming that the competitor infringes its trademark and request the ISP to remove the listing of goods. If the competitor is authorized to use the trademark and the seller send the false notification, the seller shall compensate the competitor for the damage from the Black Friday sale. If the seller is not the trademark owner and maliciously sends a false notification against its competitor, the compensation is doubled for the damage from the Black Friday sale.

In sum, the E-commerce Law requires ISPs to establishes a unified N&T system to actively prevent IP infringements. Moreover, it also develops a counter notification rule and a false notification rule to prevent the abuse of the N&T system. However, this unified IP protection system of ISPs is incomplete and demands further improvements. For example,

---

[471] Hangzhou Internet Court (杭州互联网法院), Provisions on the Electronic Evidence platform of the Hangzhou Internet Court (Trial Implementation) [杭州互联网法院电子证据平台规范(试行)], art. 4. Available at https://www.netcourt.gov.cn/portal/main/domain/lassen.htm?lang=En#lassen/litigationDocuments (last visited Nov. 25, 2018).

[472] E-commerce Law, art. 42 para. 3.

[473] E-commerce Law, art. 42 para. 3: "If a notification error causes damage to operators doing online businesses over e-commerce platform, any party concerned shall bear civil liability in accordance with the law. Anyone who sends a false notification with malicious intent, causing operators doing online businesses over e-commerce platform to incur loss, the violator shall be liable for double compensation."

Article 42 of the E-commerce Law merely provides the general principle of the false notification. This section discusses the drawbacks of the unified IP protection system of ISPs below and proposes several suggestions for the Chinese legislation and judicial branch for legal reforms.

b. Drawbacks of the unified IP protection system of ISPs

First, although the E-commerce Law sets up a false notification rule to prevent the abuse of the N&T system, it does not define the term "false notification" nor the term "malicious intent." In other words, it is unclear what constitutes a false notification under the E-commerce Law, which creates huge legal uncertainties on the unified IP protection system of ISPs. For example, if a seller plans to sell a used "Tiffany" jewelry on Taobao, and Tiffany sends a notification to Taobao claiming that the seller is selling unauthorized Tiffany jewelry, whether this notification constitutes a false notification under Article 42 of the E-commerce Law is controversial. Because of the ambiguity of Article 42, how the false notification rule will impact the ISPs in China is unclear.

In *Taobao*, the plaintiff searched potential infringing listings based on whether the price of listing was too low or the sale of listing was authorized. However, Taobao claimed that approximately 20% of the notifications sent from the plaintiff were not involved with trademark infringements, which caused damage to the sellers and the goodwill of Taobao.[474] Hypothetically, if Article 42 of the E-commerce could be applied to this case, the court has to figure out: (1) whether the notification error of the plaintiff caused damage to the seller of Taobao, (2) whether the notification error of the plaintiff constituted false notification, and (3) whether the plaintiff sent out notification with malicious intent. Because these issues are unclear under the current Article 42 of the E-commerce Law, this dissertation suggests that the

[474] *Taobao*, at 1.

Supreme People's Court should publish a judicial interpretation to further explain the legal issues concerning the false notification rule.

Second, whether the E-commerce Law imposes too many duties on the ISPs is controversial. At a press conference held by the General Office of the NPC Standing Committee after the E-commerce Law was promulgated, Yin Zhongqing, the vice chairman of Financial Affairs Committee, said that "the law … covers not only famous platforms such as Alibaba's Taobao but also those selling goods via social networks including the popular chatting app WeChat."[475] In other words, even though WeChat is merely a chatting app, it shall bear the same IP protection duties like the online retailer giant Taobao. However, for startup companies that provide online platforms, even though they are aware that their platforms can be used to sell goods, it is impossible for them to establish a N&T system such as Alibaba's AIPP platform. Therefore, the E-commerce Law may impose too many duties on startup ISPs and chill the development of the Internet Industry in China.

c. Conclusion

In conclusion, the E-commerce Law adopts an active-preventive approach and establishes a unified IP protection system of ISPs. This active-preventive approach might impose on intermediaries a greater obligation to engage in affirmative steps to prevent future infringement (depending upon assessment of costs and benefits).[476] Before the E-commerce Law, even though China adopted a passive-reactive approach of ISPs and provided a DMCA-like model of ISPs in different laws and regulations, the IP infringement issues remained serious for decades. As Yin Zhongqing explained at the press conference, the E-commerce Law aggravated the legal duties of ISPs based on the practical facts of the national conditions of China.[477] In the last decade, the trademark infringement and unfair competition issues of ISPs

[475] Yan, *supra* note 101.
[476] DINWOODIE, *supra* note 385, at 27.
[477] NPC Standing Committee (全国人大常委会), *Press conference of the General Office of the NPC Standing*

remained serious because the passive-reactive model of ISPs did not provide sufficient incentive for ISPs to prevent IP infringements. Hence, the Chinese legislation set up an active-preventive model in order to compel ISPs to actively protect IP in E-commerce Law. Although the argument is that the E-commerce Law may impose too much burden on ISPs, an active-preventive model of ISPs might be an appropriate approach to solve the serious IP infringement issues of ISPs in China.

Committee (2018.08.31) (全国人大常委会办公厅 2018 年 8 月 31 日新闻发布会) *supra* note 102.

Chapter V: Proposal for the legal reform

This Chapter introduces several legal solutions for the issues of ISPs, including the Graduated Response and the Website Blocking Injunction. Part A introduces the background of an active-preventive approach of ISPs. Part B analyzes the advantages and drawbacks of the Graduated Response and discusses whether China should adopt this policy for copyright protection. Part C examines recent legal reforms and cases of the blocking injunction, and explores whether China should adopt this policy to improve its IP mechanism. Part D concludes a proposal for China to consider adopting a government-supervised blocking injunction system or a court-supervised blocking injunction system.

A. Background

If IP holders discover unauthorized material on the Internet, there are three means for them to seek to enforce their IP rights: (1) They can pinpoint the direct infringer who is liable for disseminating the infringing materials and take action against the infringer; (2) They can send a notification to ISPs and seek to remove the infringing material under the N&T procedure; and (3) They can "block or restrict end users from assessing the material."[478] As mentioned before, the first method may be costly and impracticable because the direct infringer is anonymous and widespread on the Internet. The second method follows a passive-reactive approach that provide a safe harbor for ISPs, such as the DMCA. For example, Section 512 requires ISPs to set up an N&T system for IP protection.[479] Because the N&T systems established by ISPs are private and extrajudicial, the effectiveness of the N&T systems are questionable. The third method follows an active-preventive approach that requires ISPs to

[478] JAANI RIORDAN, WEBSITE BLOCKING INJUNCTION UNDER UNITED KINGDOM AND EUROPEAN LAW 275 (Graeme B. Dinwoodie ed., Springer 2017).
[479] 17 U.S.C. § 512(c)(1), See also 17 U.S.C. § 512 (d).

actively prevent IP infringement. For instance, Article 41 of the E-commerce law adopt this approach by requiring ISPs to actively cooperate with IP holders for IP protection.[480] Namely, IP holders can require the ISPs to cooperate and use technical means to prevent end users from retrieving the infringing materials.[481] Hence, other than the N&T procedure, the E-commerce Law provides an alternative means for IP holders to actively prevent IP infringement. According to Article 43, after receiving the infringement notifications from IP holders, the ISPs shall inform the IP holders to "file a complaint with the relevant competent department or a lawsuit with the people's court."[482] However, the E-commerce law does not provide further detail on how the people's courts or administrative departments shall solve the IP disputes of ISPs.

As a proposal for Chinese legislation to improve the active-preventive model of ISPs, this section introduces two polices within this approach: The Graduated Response and the Website Blocking Injunction. Because whether China should adopt these polices into system of ISPs is controversial, this section first analyzes the advantages and drawbacks of these two policies, and then concludes with an analysis on whether Chinese administration or legislation should adopt these polices.

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,"[483] which reflects how it terminates people's Internet connection. In the

[480] E-commerce Law, art. 41.
[481] RIORDAN, *supra* note 478, at 276.
[482] E-commerce Law, art. 43 para. 2.
[483] WILLIAM PATRY, MORAL PANICS AND THE COPYRIGHT WARS 14 (Oxford University Press, 1st ed. 2009).

EU, the Graduated response is also called "Three Strikes disconnection policies."[484] 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 superior administrative authority, the High Authority for the Dissemination of Works and the Protection of Rights on the Internet (HADOPI), to regulate its graduated response policy. The Creation and Internet Act came into effect on January 1, 2010.[485] So far, the Graduated Response law exists in some countries, but in the past has not been norm.[486]

Even though the Graduated Response may not be a legal requirement, ISPs can adopt it to prevent online copyright infringement. For example, Indiana University (IU) adopted the Graduated Response policy in its online safety & security policy.[487] 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, when IU receives a N&T notification from the copyright owner, the IT department of IU would disable the infringer's access to IU wireless network

---

[484] 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).

[485] LOI no 2009-669 du 12 juin 2009 favorisant la diffusion et la protection de la cr6ation 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 Rdpublique Frangaise [J.0.] [Official Gazette of France], June 12, 2009, p. 9666, available at http://legifrance.gouv.fr/affichTexte.do;jsessionid=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.'"

[486] JEREMY & CHRISTOPHER, *supra* note 32, at 388.

[487] Indiana University, *Copyright tutorial* IU, https://protect.iu.edu/online-safety/personal-preparedness/file-sharing/tutorial.html (last visited Oct. 25, 2016).

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.[488] If the infringing activity occurs three times, in additional 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.

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 the Graduated Response terminates repeated infringers. However, Internet users may complain about the Graduated Response procedure after receiving warnings from ISP because they are concerned about being disconnected from the Internet.[489] The next section discusses whether China should adopt this policy and analyzes the advantages and drawbacks of the Graduated Response procedure.

2. Advantages

First, the Graduated Response system can help ISPs avoid the constant need to respond to lawsuits and the high costs of legal defense,[490] which is a cure for massive amounts of copyright infringement issues in China. As mentioned in Chapter II, China has launched a month-long anti-piracy campaign every year since 2010.[491] In 2017, the NCAC launched "Sword Net Campaign" to tackle online copyright infringement and Chinese law enforcement departments shut down 2554 infringing piracy websites, blocked 0.710 million infringing

[488] Indiana University, *Copyright infringement incident resolution* IU, https://protect.iu.edu/online-safety/personal-preparedness/file-sharing/violations.html (last visited Oct. 25, 2016).
[489] HUA, *supra* note 105, at 123.
[490] *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).
[491] Jiang Jie, China highlights IPR protection to encourage creativity, People's Daily Online, (12:03, Aug. 23, 2018) available at http://en.people.cn/n3/2018/0823/c90000-9493519.html (last visited Oct. 23, 2018).

piracy links, captured 2.76 million infringing piracy products, amounting to RMB 107 million (approximately USD 15.6 million).[492] By adopting the Graduated Response system, ISPs may avoid being scapegoats for their users' infringing activities.[493] Consequently, ISPs may spend more resources on developing and improving its network services instead of handling lawsuits.

Second, the Graduated Response may facilitate the cooperation between ISPs and copyright owners.[494] Article 41 of the E-commerce law requires ISPs to cooperate IP owners and establish IP protection rules, and adopting the Graduated Response provides an alternative mechanism to fight Internet piracy. In addition, the Graduated Response goes beyond a traditional passive-reactive approach and implies an educational notification mechanism for alleged online infringers before more stringent measures can be imposed.[495] In *Baidu* and *SOHO*, the People's Courts held that the ISP should pay a duty of care to online infringement and adopt effective measures to prevent infringement.[496] Therefore, adopting the graduated response is an alternative solution for Chinese ISPs to fulfill the legal requirements.

Third, as Professor Strowel elaborated, the Graduated Response system has educative and rehabilitative benefits.[497] 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.[498] Most of the Internet users pay no respect to copyright and disseminates infringing copyrighted works through ISPs. Adopting the Graduated Response may be an effective and publicly acceptable way to raise awareness of copyright law in the Chinese society.

---

[492] NCAC (国家版权局), *Report of the "Sword Net Campaign 2017,"* ("剑网 2017"专项行动的有关通报), *supra* note 80.
[493] Peter K. Yu, *The Graduated Response*, 62 FLA. L. REV. 1373, 1384 (2010).
[494] *Id.*
[495] 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).
[496] *Baidu*, Beijing High People's Ct., *supra* note 147, at 25.
[497] Strowel, *supra* note 215, at 86.
[498] HUA, *supra* note 105, 129.

3. Drawbacks

The first drawback of the Graduated Response system is that it is costly to ISPs by raising the costs of surveillance, policing, and date retention. Such financial burden may cause ISPs to stop improving their network or offering low-cost services.[499] In *SOHO*, even though the defendant Hode merely provided link service to legitimate ISPs, the Shanghai IP court held that link service providers should bear duty of care on whether the linked contents were legitimate. If ISPs are required to adopt the Graduated Response, it is likely that Hode may stop providing its link service due to the financial burden. Although the financial burden might not be a problem for giant technology companies, it could be fatal for any start-up or small ISPs.[500]

Second, although the Graduated Response procedure is an alternative solution for copyright protection in China, the Chinese legislature is prudent on legally transplanting this policy because implementing a new Graduated Response mechanism may bring an adverse effect to Internet users in China. As mentioned before, online copyright infringement is a serious issue in China and most Internet users in China do not even know or even care about copyright protection. Applying the 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."[501] Therefore, it is too controversial for the Chinese legislature to enact the Graduated Response procedure into law.

Third, Chinese government is prudent on adopting the Graduated Response policy because terminating Internet connection is the opposite of promoting online government

[499] Yu, *supra* note 213, 1391-1392.
[500] EMARKETER, *supra* note 91.
[501] PATRY, *supra* note 483, at 14.

services. Since Chinese Premier Li Keqiang raised the "Internet Plus governance" strategy in the 2016 government report,[502] the State Council of the PRC published multiple guidance to local governments and departments and require them to build websites and information platforms, and constantly optimize online administrative services.[503] Moreover, Chinese government also cooperates with the giant ISPs and provide government services through their platforms, such as WeChat and Alipay. Hence, adopting the Graduated Response policy may create unnecessary conflict against the Chinese government strategy.

4. Conclusion

Adopting Graduated Response procedure may effectively punish repeated online infringers and prevent the copyright infringement, but it is also controversial and is not suitable for all ISPs. Although ISPs that are overwhelmed by copyright infringements may obtain significant effect on copyright protection by adopting the Graduated Response procedures, terminating Internet connection may create a chilling effect on their users. Moreover, terminating Internet connection is also the opposite of the "Internet Plus governance" strategy in China. As a result, neither the Chinese legislation or government nor Chinese ISPs show strong interests in implementing the Graduated Response policy.

C. The Website Blocking Injunction

1. Introduction

The Website Blocking Injunction is a court-supervised mechanism that originated in the EU, and lately adopted and developed in Singapore and Australia. Unlike the extrajudicial

[502] www.gov.cn (中华人民共和国中央人民政府) China's focus on Internet Plus governance, (Feb. 1, 2017, 09:17), available at: http://english.gov.cn/premier/news/2017/02/01/content_281475556331388.htm.
[503] www.gov.cn (中华人民共和国中央人民政府), Measures taken to promote Internet Plus government service, (Aug. 18, 2017, 02:13 PM), available at: http://english.gov.cn/premier/news/2017/08/18/content_281475798536474.htm.

N&T systems that are commonly established by ISPs, the blocking injunction is a court order that compel Internet apparatus providers (e.g. China Telecom, China Mobile or China Unicom) that provide Internet connection services to block access to Internet locations where infringing content resides. The blocking injunction reduces the impact of infringement by hiding the infringing content from internet users residing in the country where an Internet apparatus provider operates.

In the EU, the N&T mechanism applies to ISPs such as Internet content providers, compelling them to block alleged infringing content hosted or linked by them. While the blocking injunction has been used to control the conduct of ISPs such as Internet apparatus providers, compelling them to block access to alleged infringing content.[504] The legal basis for blocking injunctions in the EU is supplied by Article 8(3) of the InfoSoc Directive (2001/29):[505]

> Member States shall ensure that right holders are in a position to apply for an injunction against intermediaries whose services are used by a third party to infringe a copyright or related right.

Following this principle, some EU Member States such as the United Kingdom (UK) before exiting the EU, implemented the blocking injunction provision in Section 97A to the Copyright Designs and Patent Act 1988 (CDPA). It allows the High Court of England and Wales to grant an injunction against an ISP that has actual knowledge of another person using its service to infringe copyright.[506]

Other jurisdictions such as Australia also adopted the Website Blocking Injunction in the amendment of Copyright Act 1968 (Cth). Australia amended the Copyright Act 1968 (Cth) in 2015 and introduced the Copyright Amendment (Online Infringement) Act 2015

[504] Althaf Marsoof & Dr Aipana Roy, The Blocking Injunction: A Comparative and Critical Review of the EU, Singaporean and Australian Regimes, 38 Eur. Intell. Prop. Rev. 92 (Issue 2) (2016), at 634.
[505] Directive 2001/29 on the harmonisation of certain aspects of copyright and related rights in the information society (InfoSoc Directive).
[506] Copyright Designs and Patent Act 1988, Section 97A.

(Commonwealth), which is also called the Online Access Disabling Provisions (hereinafter "OADP"). The OADP came into effect on 27 June 2015 and Section 115A(1)[507] allows the Federal Court with jurisdiction to grant blocking injunctions against ISPs. Before the issuance of an injunction, which compels an ISP to block access to a particular online location that infringes copyright, the court must be satisfied that:

> (a) a carriage service provider provides access to an online location outside Australia; and
> (b) the online location infringes, or facilitates an infringement of, the copyright; and
> (c) the primary purpose of the online location is to infringe, or to facilitate the infringement of, copyright (whether or not in Australia).[508]

According to the Explanatory Memorandum issued by Australian House of Representatives, the blocking injunction is a no-fault remedy that neither affects existing laws nor creates a presumption on the infringement of ISPs.[509] To further explain how the court applies the OADP, a case of the blocking injunction in Australia will be analyzed below.

2. Roadshow Films Pty Ltd. v. Telstra Corporation Ltd.

a. Background

Roadshow[510] is the first Website Blocking Injunction case in Australia. The plaintiffs were copyright owners such as Roadshow films, who found large numbers of their copyrighted works infringed by various online locations outside Australia. The plaintiffs brought proceedings against defendants, ISPs such as Telstra that provided Internet connection services in Australia, and sought blocking injunction orders under the OADP that disable access to various online locations involved in copyright infringement activities.[511]

b. 115A(1)(a)

When applying OAPD to grant a blocking injunction order, the court first analyzed

[507] Copyright Act 1968 (Cth), s 115A(1).
[508] Copyright Act 1968 (Cth), s 115A(1).
[509] Explanatory Memorandum, Copyright Amendment (Online Infringement) Bill 2015 (Cth), 2 (Austl.).
[510] Roadshow Films Pty Ltd v Telstra Corporation Ltd [2016] FCA 1503 (Austl.).
[511] *Roadshow*, at [1].

three requirements in Section 115A(1). Regarding the first element that requires an ISP provide access to the Internet, the court confirmed that defendants constituted carriage service providers (i.e. ISPs) under Section 87(1) of the Telecommunications Act because these ISPs provided access to online locations outside Australia. Although the term "online location" is not defined in the Copyright Act 1968 (Cth), the Explanatory Memorandum noted that "'online location' is intentionally broad and includes, but is not limited to, a website, and would also accommodate future technologies."[512] In this case, the online locations involved copyright infringement referred to the primary or proxy servers outside Australia.

c. 115A(1)(b)

Regarding to the second requirement that requires the online location infringes copyright or facilitates copyright infringement, the court first confirmed the exclusive rights of the plaintiffs under Section 86,[513] and their copyrighted works were infringed on online locations outside Australia without authorization under Section 101.[514] Second, the court held that even though it was impossible to find the person who operated the online locations or made content available online, Section 115A permitted the grant of an injunction.[515] Third, the court analyzed the online locations infringed copyright based on direct and secondary infringement theories that were similar to the infringement theories in *YouTube* and *SOHO*. The court concluded that even if the online locations did not themselves infringe copyright, it might facilitate the infringement by making it easier for users to ascertain the existence or whereabouts of other online locations that involved direct or secondary infringement.[516]

---

[512] Explanatory Memorandum, Copyright Amendment (Online Infringement) Bill 2015 (Cth), 8 (Austl.).
[513] Copyright Act 1968 (Cth), s 86.
[514] Copyright Act 1968 (Cth), s 101: "Subject to this Act, a copyright subsisting by virtue of this Part is infringed by a person who, not being the owner of the copyright, and without the licence of the owner of the copyright, does in Australia, or authorizes the doing in Australia of, any act comprised in the copyright."
[515] *Roadshow*, at [46].
[516] *Roadshow*, at [47].

d. 115A(1)(c)

According to the Explanatory Memorandum, the third requirement of Section 115A(1) is also called the "primary purpose test" that is "an intentionally high threshold for the copyright owner to meet as a safeguard against any potential abuse."[517] The court concluded that in order to prove the primary purpose of the online location to infringe copyright or facilitate the infringement of copyright, "the principal activity for which the online location is used or designed to be used is copyright infringement or the facilitation of copyright infringement."[518] Therefore, ISPs such as YouTube that are routinely used by users to infringe copyright does not establish that the primary purpose of YouTube is to infringe copyright or facilitate infringement.

e. The scope of a blocking injunction

After analyzing three requirements for a blocking injunction order, an issue regarding to the scope of an order was raised in court. Because the online locations involved copyright infringement may change their domain names, IP addresses or URLs to avoid supervision of copyright owners, the scope of a blocking injunction that was granted by a court may not cover additional online locations via different or new domain names, IP addresses or URLs. Thus, the plaintiffs asserted to extend the scope of an order by providing written notice to the defendants so that the ISPs can easily re-establish a blocked website without further legal process.[519]

The court disagreed with the plaintiffs' assertion and held that "[w]hether the terms of any injunction should be varied to refer to additional Domain Names, IP Addresses or URLs is a matter for the Court to determine in light of evidence."[520] By simply submitting a notification

[517] Explanatory Memorandum, Copyright Amendment (Online Infringement) Bill 2015 (Cth), 9 (Austl.).
[518] *Roadshow*, at [49].
[519] *Id*, at [136].
[520] *Id*, at [137].

to ISPs and providing additional blocking online locations, the additional online locations may not point to any of the same online locations in relation to the original injunction.[521] Therefore, The plaintiff's proposal may grant copyright owners too much power to block additional online locations without supervision of a court.

f. Summary

The Website Blocking Injunction mechanism provides a new way for copyright owners to fight against online piracy. Unlike the N&T mechanism, the copyright owners can actively protect their works through a court-supervised mechanism. The legal experience from Australia provides a valuable reference for developing countries that are strengthening copyright protection. Introducing this mechanism into China is consistent with a trend of an active-preventive approach to protect copyright owners against online infringement. Section B below analyzes whether China should adopt the blocking injunction mechanism into its IP protection system.

D. Proposals for the legal reform in China

The E-commerce law provides a legal foundation for China to adopt new IP protection systems. Other than N&T system, Article 43 of the E-commerce law provides two alternative ways for IP owners to protect their rights: (1) filing a complaint to an administrative department; and (2) filing a lawsuit to a people's court. Although the E-commerce law does not provide further guidance on how administrative departments or people's courts should solve IP issues, China can adopt the Website Blocking Injunction mechanism to strengthen its IP protection based on Article 43. This dissertation suggests that the Chinese legislation can adopt the blocking injunction mechanism into (1) administrative regulations to establish a government-

[521] *Id*, at [138].

supervised system, or (2) laws or regulations to establish a court-supervised system.

1. A government-supervised blocking injunction system

Compared to a court-supervised system, it is easier for China to establish a government-supervised blocking injunction system because (1) Article 5 of the E-commerce law comply ISPs to protect IP rights and accept the supervision of the government;[522] and (2) China has already established an effective Internet censorship system. The Internet censorship requirements are mandatory for ISPs in China, and even giant technology companies such as Google considered providing a censored version of its services in order to return to the Chinese online market.[523] This Internet censorship system is called the "Great Firewall," which is one of the world's most sophisticated system for controlling and surveilling the web.[524] Because Article 6 paragraph 12 of the People's Police Law of the PRC[525] grants Chinese police the power to "supervise and administer the work of protecting the computer information system,"[526] the Ministry of Public Security of the PRC launched the "Golden Shield Project" to monitor and secure cyberspace in China.[527] The Great Firewall system was developed from the Golden Shield Project. Based on the Regulations of the PRC for Safety Protection of Computer Information Systems,[528] multiple Chinese government departments,[529] such as the

---

[522] E-commerce law, art. 5.
[523] Heather Kelly, *Google's CEO says it's still considering a censored search engine in China*, CNN (Oct. 16, 2018 12:14 A.M.) https://www.cnn.com/2018/10/15/tech/google-china-sundar-pichai/index.html.
[524] James Griffiths, China is exporting the Great Firewall as internet freedom declines around the world, CNN. https://www.cnn.com/2018/11/01/asia/internet-freedom-china-censorship-intl/index.html.
[525] Zhong hua ren min gong he guo jing cha fa (中华人民共和国警察法) [People's Police Law of the PRC] (promulgated by the Standing Comm. Nat'l People's Cong., Feb. 28, 1995, amended by the Standing Comm. Nat'l People's Cong., Oct. 26, 2012, effective in Jan. 1, 2013) (China). Translated by Westlaw china (www.westlawchina.cn).
[526] People's Police Law of the PRC, art. 6 para 12.
[527] Xiao Qiang, *How China's Internet Police Control Speech on the Internet*, (Nov. 24, 2008) Radio Free China. Available at https://www.rfa.org/english/commentaries/china_internet-11242008134108.html.
[528] Zhong hua ren min gong he guo ji suan ji xin xi an quan bao hu tiao li (中华人民共和国计算机信息安全保护条例) [Regulations of the People's Republic of China for Safety Protection of Computer Information Systems] (promulgated by the State Council, Feb. 18, 1994, amended by the State Council, Jan. 8, 2011, effective in Feb. 18, 1994) (China). Translated by Westlaw china (www.westlawchina.cn).
[529] Regulations of the People's Republic of China for Safety Protection of Computer Information Systems, art. 6: "The Ministry of Public Security shall be in charge of the nationwide safety protection work of computer information systems.
The Ministry of State Security, the National Administration for the Protection of State Secrets and other

Ministry of State Security and the National Administration for the Protection of State Secrets, cooperated and developed the Great Firewall for Internet censorship. According to the Administrative Measures on Internet Information Services,[530] the main purpose of the Great Firewall is to prevent ISPs from disseminating harmful information, such as national security and government secrets.[531] Although the Internet censorship system is not designed to protect IP, it may become a powerful technological measure for China to establish a government-supervised Blocking Injunction system for IP infringements.

First, from a technical perspective, the Great Firewall provides sufficient technical support to establish a blocking injunction system. Although the Chinese authorities have never released any technical details about the Great Firewall, IT experts outside China considered the Great Firewall as one of the largest, most extensive, and most advanced Internet censorship system in the world.[532] The Great Firewall adopts multiple techniques to scan URLs, detect web page content and block websites.[533] Even if the infringing websites, such as Pirate Bay in *Roadshow*, changes domain names, IP addresses or URLs in order to continue infringing activities,[534] the Great Firewall is capable of anti-circumvent by DNS poisoning, blocking

---

departments concerned under the State Council shall properly perform the relevant functions related to the safe protection of computer information systems within the scope of their competence and responsibilities stipulated by the State Council."

[530] Hu lian wang fu wu guan li ban fa (互联网服务管理办法) [Measures on Internet Information Services] (promulgated by the State Council, Sep. 25, 2000, amended by the State Council, Jan. 8, 2011, effective in Sep. 25, 2000) (China). Translated by Westlawchina (www.westlawchina.cn).

[531] Measures on Internet Information Services, art. 15: An Internet information service provider shall not produce, reproduce, publish or distribute information containing the following content that:
(1) Opposes the cardinal principles determined in the Constitution;
(2) Compromises the State security, divulges the State secrets, subverts State power, or undermines the unity of the nation;
(3) Damages the honor and interests of the nation;
(4) Incites ethnic hatred or racial discrimination or undermines the national solidarity;
(5) Sabotages the religious policies of the State, propagates heresies or superstition;
(6) Disseminates rumors, disrupts the social order or undermines the social stability;
(7) Disseminates obscenity, pornography, gambling, violence, murder, horror or instigates others to crime;
(8) Infringes others' legitimate rights and interests by insulting or slandering others; or
(9) Is otherwise prohibited by the laws or administrative regulations.

[532] Chris Hoffman, *How the "Great Firewall of China" Works to Censor China's Internet*, Howtogeek (Sep. 22, 2016), https://www.howtogeek.com/162092/htg-explains-how-the-great-firewall-of-china-works/ (last visited Nov. 24, 2018).

[533] Hoffman, *supra* note 532.

[534] *Roadshow*, at [81]-[105].

access to IP addresses, analyzing and Filtering URLs.[535] Moreover, even if the Internet users try to access infringing websites through VPN, which is one of the most effective way to circumvent the Great Firewall, the Great Firewall is capable of identifying encrypted VPN traffic and even terminating the VPN connection.

Second, from a policy perspective, the Chinese legislation may follow the "Internet Plus governance" policy and consider adopting a government-supervised blocking injunction system. According to the guideline issued by the State Council on Sep. 2016, the purpose of promoting the "Internet Plus governance" policy is to strengthen government supervision, optimize online service, stimulate market vitality and social creativity.[536] Following the "Internet Plus governance" policy, the Network Security Law was promulgated in November 2016. One of the main purposes of the law is international cooperation such as cyberspace governance, fighting against online illegal and criminal activities.[537] Notably, not only does Article 12 of the Network Security Law follow Article 15 of the Administrative Measures on Internet Information Services and stipulates that ISPs and network users shall not "endanger national security,"[538] but it also provides that ISPs and network users shall not infringe intellectual property rights.[539] Thus, a government-supervised blocking injunction system will follow the network policy in China and strengthen government supervision on cybercrime. Moreover, it improves the IP protection system by promoting IP governance in China. Furthermore, because China's position is that national governments have the ultimate right to control the internet within their borders,[540] it is possible for the Chinese government to

---

[535] *Id*.
[536] www.gov.cn (中华人民共和国中央人民政府), *China's focus on Internet Plus governance*, (Feb. 1, 2017, 09:17), available at: http://english.gov.cn/premier/news/2017/02/01/content_281475556331388.htm (last visited Nov. 18, 2018).
[537] Network Security Law, art. 7.
[538] Network Security Law, art. 12 para. 2.
[539] Network Security Law, art. 12 para. 2.
[540] James Griffiths, *China is exporting the Great Firewall as internet freedom declines around the world*, CNN. https://www.cnn.com/2018/11/01/asia/internet-freedom-china-censorship-intl/index.html.

establish a government-supervised blocking injunction system and implement it into the Internet censorship system.

Third, from a legal perspective, the Chinese legislation may grant administrative power to government departments in order to establish a government-supervised blocking injunction system. Article 6 of the E-commerce Law stipulates that: "[t]he relevant departments of the State Council shall be responsible for the promotion, supervision and administration of electronic commerce according to the division of responsibilities."[541] Moreover, according to Article 77 of the Draft of the Third Amendment of the Copyright Law, the Copyright Administrative Department is authorized to stop activities of copyright infringement.[542] Following Article 77, the Chinese legislation may establish a government-supervised blocking injunction system and enact it into different administrative regulations. By following the administrative regulations, different government departments are capable of cooperating and implementing a government-supervised blocking injunction system.

In conclusion, there is almost no obstacle for the Chinese legislation to establish a government-supervised blocking injunction system as long as the Chinese government decides to prevent online copyright infringement through this approach. In particular, Chinese government departments cooperated and launched a month-long anti-piracy campaign every year since 2010.[543] Although the Internet censorship system in China was not designed to protect IP, the Chinese government can turn it into a powerful firewall against online IP infringement. As a suggestion, a simple government-supervised blocking injunction system in the copyright regime can be: (1) copyright owners report suspicious copyright infringements to the NCAC and request for a blocking injunction; (2) the NCAC verifies and estimates infringing activities and decides if a blocking injunction should be issued; (4) the NCAC issues

[541] E-commerce Law, *supra* note 25, art. 6.
[542] 2014 Copyright Draft, *supra* note 30, art. 77.
[543] Jiang Jie, *China highlights IPR protection to encourage creativity*, People's Daily Online (人民网), (12:03, Aug. 23, 2018) available at http://en.people.cn/n3/2018/0823/c90000-9493519.html (last visited Oct. 23, 2018).

a blocking injunction to the Ministry of Public Security if the copyright owners' requests are approved; and (5) the Ministry of Public Security orders the Public Information Network Security and Monitoring Bureau that operates the Great Firewall to block the infringing websites.

2. A court-supervised blocking injunction system

Compared to establishing a government-supervised blocking injunction system, it seems that the Chinese legislation is not incentivized to establish a court-supervised blocking injunction system. At least, it is unlikely for the Chinese legislation to establish a court-supervised blocking injunction system in the Third Amendment of the Copyright Law. The main reason is because the Draft of the Third Amendment of the Copyright law does not include any provisions related to the blocking injunction order. In order to enact a court-supervised blocking injunction system into law, relevant provisions have to be drafted and submitted to the Standing Committee of the NPC for deliberation. According to Article 83, the draft merely provides that for cases that involve copyright or copyright-related rights infringement, the people's court may confiscate the illegal gains, the infringing products or reproductions, and the property used in the illegal activities.[544]

Although it is almost impossible for the Chinese legislation to establish a court-supervised blocking injunction system in the Third Amendment of the Copyright Law, the Chinese legislation may consider legally transplanting a court-supervised blocking injunction system, such as the OADP of Australian Copyright Act, into IP protection systems for trial implementation in the future. The Supreme People's Court is likely to assign two types of specialized courts, either the Internet Court or the IP Court, to hear cases of online IP infringement and establish a blocking injunction system for trial implementation.

[544] 2014 Copyright Draft, *supra* note 30, art. 83.

a. Internet Court

Because Internet Courts are primary people's courts that have jurisdiction on Internet-related cases such as online copyright or trademark disputes,[545] the Supreme People's Court is likely to establish a court-supervised blocking injunction system for trial implementation in the Internet Court. In August 2017, China set up the first Internet Court in Hangzhou because of the increasing number of online disputes.[546] Most of these online disputes are related to Alibaba,[547] which owns one of the biggest e-commerce platforms such as Taobao in the world. In September 2018, two more Internet Courts were set up in Beijing and Guangzhou.[548] According to the Supreme People's Court, China plans to set up more Internet Courts in areas where Internet industry is well-developed.[549] As a result, it is possible that the Chinese legislation may set up a court-supervised blocking injunction system by assigning Internet Courts to hear massive amounts of online copyright disputes.

Compared to the local people's courts that follow a traditional trial mechanism, Internet Courts are more advantageous to establish a court-supervised blocking injunction system. First, Internet Courts adopt a new online trial mechanism for trial implementation, which is called "online trial of online case."[550] Online trial mechanism is originated from Online Dispute Resolution (ODR), a method used by ISPs such as eBay, to resolve disputes arise from online

---

[545] Zui gao ren min fa yuan guan yu hu lian wang fa yuan shen li an jian ruo gan wen ti de gui ding (最高人民法院关于互联网法院审理案件若干问题的规定) [Provisions of the Supreme People's Court on Several Issues Concerning Trial of Cases by the Internet Courts] (promulgated by the Supreme People's Court, Sep. 6, 2018, effective in Sep. 7, 2018) (China) Fa Shi (2018) No. 16 [法释(2018)16 号], art. 2 item (4)&(5). Translated by Westlawchina (www.westlawchina.cn).

[546] Qin Han (秦汉), Research on Dispute Resolution Mechanism of China's Internet Court (互联网法院纠纷处理机制研究), Electronics Intellectual Property (电子知识产权), at 115. No. 10, 2018.

[547] The headquarter of the Alibaba Group Holding Limited is located in Hangzhou.

[548] Xinhua (新华网), China to launch Internet courts in Beijing, Guangzhou, (07:53, July 26, 2018), available at http://en.people.cn/n3/2018/0726/c90000-9484769.html (last visited Nov. 23, 2018).

[549] Notice of the Supreme People's Court on Issuing the Plan for Adding the Beijing Internet Court and the Guangzhou Internet Court (最高人民法院印发《关于增设北京互联网法院、广州互联网法院的方案》的通知) No. 216 (2018) [法(2018)216 号], at 1.

[550] Hangzhou Court of the Internet, Network Copyright Judicial Protection Report (April 2018), at 1. http://hztl.zjcourt.cn/ (last visited Nov. 3, 2018).

transactions.[551] The Internet Courts adopted several ideas from ODR such as Online Negotiation, Online Mediation, Online Arbitration and Online Justice, and developed ODR to a new online trial mechanism.[552] For example, the Hangzhou Court of the Internet (hereinafter "Hangzhou Internet Court") established an online litigation platform to make available a series of steps of the litigation process online.[553] This online litigation process includes filing complaints, case filing approval, service of process, mediation, evidence submission, direct examination, cross-examination, pre-trial preparation, court-hearing, pronouncing judgement and enforcement.[554] Because most of the online copyright infringement cases involves ISPs that are not IP experts, online trial mechanism provides an impartial, efficient and convenient way to resolve various Internet-related disputes.

Second, Internet Court adopts a new online trial mode for trial implementation, which is called "asynchronous trial." Hangzhou Internet Court defines asynchronous trial in the "Rule on Asynchronous Trial related to Internet cases," which means that different steps of trial process are divided and distributed on the online litigation platform. The Judge, plaintiff and defendant can log into the online litigation platform at different times, and finish the requirements of the trial process within a given period.[555] For example, if the copyright owner of Star Wars in the U.S. discovers a seller who sells backpacks printed with Star Wars images without authorization on Taobao, the copyright owner can sue the seller on the online litigation platform of Hangzhou Internet Court without traveling to China. Due to the geographic

---

[551] See e.g. https://pages.ebay.com/services/buyandsell/disputeres.html.

[552] Shu Yihong (疏义红) & Xu Jisheng (徐记生), From the Online Dispute Resolution to the Internet Court (从在线争议解决到互联网法院), People's Court Daily (人民法院报), Nov. 11, 2017.

[553] www.netcourt.gov.cn(杭州互联网法院诉讼平台), English vision is available at http://www.netcourt.gov.cn/portal/main/domain/index.htm?lang=En.

[554] Hangzhou Court of the Internet (杭州互联网法院网上庭审规范), The Trial Procedure of the Litigation Platform of Hangzhou Internet Court (杭州互联网法院网上庭审规范), art. 2. English vision is available at https://www.netcourt.gov.cn/portal/main/domain/lassen.htm?lang=En#lassen/litigationDocuments (last visited Nov. 25, 2018).

[555] Hangzhou Court of the Internet (杭州互联网法院), Rule on Asynchronous Trial related to Internet cases (trial implementation) [涉网案件异步审理规程(试行)], at 1. Available at https://www.netcourt.gov.cn/portal/main/domain/lassen.htm#lassen/litigationDocuments.

distance and time lag, the copyright owner can apply for asynchronous trial, such as submitting electronic evidence within one week, or cross-examination by leaving messages on the online litigation platform within two weeks. As a result, the asynchronous trial provides an effective way to resolves online copyright disputes without limitation of space-time.

Third, because the Supreme People's court is exploring the establishment of a unified litigation platform, the Internet Courts are potential to become a nexus for administrative organizations and major ISPs.[556] According to the data from the Hangzhou Internet Court, almost forty percent of cases are online copyright infringement cases, and nearly sixty percent of these cases are resolved online.[557] This data shows a trend that both ISPs and Internet users tend to resolve online copyright disputes through Internet Courts instead of local people's courts. Therefore, this dissertation suggests the Supreme People's Court to consider publishing a judicial interpretation, which establishes an online blocking injunction system for trial implementation in the Internet Courts.

b. IP Court

According to the Supreme People's Court, because IP Courts have jurisdiction to hear administrative cases involving copyright and trademark,[558] it is also possible for them to establish a court-supervised blocking injunction system for trial implementation in IP Courts. IP Courts are intermediate people's court that have jurisdiction to hear IP cases of first instance,[559] or IP cases of second instance from primary people's courts. The first instance

[556] Notice of the Supreme People's Court on Issuing the Plan for Adding the Beijing Internet Court and the Guangzhou Internet Court, *supra* note 549, at 1.
[557] Qin Han (秦汉), *Research on Dispute Resolution Mechanism of China's Internet Court* (互联网法院纠纷处理机制研究), Electronics Intellectual Property (电子知识产权), at 118. No. 10, 2018.
[558] Provisions of the Supreme People's Court on the Jurisdictions over Cases by Intellectual Property Courts in Beijing, Shanghai and Guangzhou, *supra* note 269, art. 1, item (2): "An intellectual property court shall govern the following cases of first instance within the jurisdictions of the municipality of its domicile: … (2) Administrative cases brought against the administrative acts involving copyrights, trademarks, unfair competition, etc. that are committed by the departments of the State Council or local people's governments at and above the county level."
[559] Provisions of the Supreme People's Court on the Jurisdictions over Cases by Intellectual Property Courts in Beijing, Shanghai and Guangzhou, *supra* note 269, art. 1.

cases of IP Courts shall be appealed to the IP tribunal of the Supreme People's Court.[560] For example, because Beijing has both IP Court and Internet Court, Beijing IP Court have jurisdiction to hear online copyright infringement cases of second instance appealed from Beijing Internet Court.[561] Because IP Courts are higher level than Internet Courts and specialized in IP, it is more likely that IP Court may establish a court-supervised blocking injunction system for trial implementation.

There are two possible ways to establish a court-supervised blocking injunction system in IP Court for trial implementation. First, the Chinese legislation could implement the Blocking Injunction system by amending copyright related regulations, such as the RPRD. Second, the Supreme People's court could implement blocking injunction the system by publishing a judicial interpretation, such as the 2012 Provision. As a suggestion, a simple court-supervised blocking injunction system in copyright regime can be: (1) copyright owners file a lawsuit against infringing websites outside China to a IP Court and request for a blocking injunction order; (2) the IP Court decides whether a blocking injunction order should be granted; (3) the IP Court issues a blocking injunction order to the Ministry of Public Security if the copyright owners' request is approved; and (4) the Ministry of Public Security orders the Public Information Network Security and Monitoring Bureau that operates the Great Firewall to block the infringing websites. In determining whether to grant the injunction, Section 115A(5) of the Australia Copyright Act provides eleven factors for the court to consider.[562] Based on the effect of the trial implementation of the court-supervised Blocking Injunction system, the Chinese legislation may consider enacting it into the Fourth Amendment of the Copyright Law.

---

[560] Zui gao ren min fa yuan guan yu zhi shi chan quan fa ting ruo gan wen ti de gui ding (最高人民法院关于知识产权法庭若干问题的规定) [Provisions of the Supreme People's Court on Several Issues Concerning Intellectual Property Tribunal] (promulgated by the Supreme People's Court, Dec. 3, 2018, effective in Jan. 1, 2019) (China), art. 1.

[561] Provisions of the Supreme People's Court on Several Issues Concerning Trial of Cases by the Internet Courts, *supra* note 545, art. 4.

[562] Copyright Act 1968 (Cth), s 115A(5).

c. Hybrid blocking injunction systems

The Chinese legislation may consider setting up a hybrid blocking injunction system for trial implementation that requires cooperation between administrative departments and the people's courts. For example, the NCAC has the power to issue blocking injunction orders against online copyright infringement, and the IP courts have jurisdiction to hear cases involving blocking injunction orders. Moreover, a hybrid blocking injunction system requires a unified platform among copyright owners, people's courts, administrative departments and major ISPs to share information, therefore, prevent copyright from online infringement. In the light of the Internet Plus governance strategy, the Supreme People's Court suggested Internet Courts to transform and improve the online litigation platform to a unified online platform for promoting online trial mechanism and sharing information.[563] Therefore, a hybrid blocking injunction system that depends on establishing a unified online platform is also a feasible program for China.

d. Conclusion

In conclusion, the Chinese legislation is likely to set up a government-supervised blocking injunction system for trial implementation before setting up a court-supervised blocking injunction system. As mentioned before, the Chinese legislation tends to legally transplant a foreign legal doctrine into administrative regulations for trial implementation first. After the trial implementation period, the Chinese legislation may consider adopting a foreign legal doctrine with modifications. For example, China first adopted the Safe Harbor doctrine and the N&T system from the U.S. Copyright Act into ICM in 2005.[564] After a one-year trial implementation, the Chinese legislation modifies the safe harbor provision and N&T provision

[563] Notice of the Supreme People's Court on Issuing the Plan for Adding the Beijing Internet Court and the Guangzhou Internet Court, *supra* note 549, at 1.
[564] ICM, *supra* note 225, art. 5.

to fit national conditions of China, and enacted them into the RPRD.[565] In 2018, the Chinese legislation adopted the safe harbor provision and N&T provision into the E-commerce law, and considered adopting them into the third amendment of Copyright Law.

Although the Chinese legislation may not set up a court-supervised blocking injunction system in the third amendment of Copyright Law, it is likely that the Supreme People's court may adopt the blocking injunction into judicial interpretation based on Article 43 of the E-commerce law. After laws or regulations coming into effect, the Supreme People's court has power to issue judicial interpretation in order to solve specific issues in cases. For example, as mentioned before in this chapter, Article 36 of the Tort Liability Law adopted the Red Flag provision from the U.S. Copyright Act, but it does not provide details on how to determine the constructive knowledge of ISPs.[566] To solve ISP related issues, the Supreme People's court issued the 2012 Provision to construe ISPs related laws and regulations, including Article 36 of the Tort Liability Law. Article 9 of the 2012 Provision lists seven factors[567] for people's court to consider when determining the constructive knowledge of ISPs, and this seven-factor test is similar to the Red Flag test in *YouTube*.

Similar to Article 36 of the Tort Liability Law, although Article 43 stipulates that IP holders can seek remedy in the people's courts outside the N&T regime,[568] the E-commerce law does not provide guidance on how the people's courts shall solve specific IP issues. Therefore, the Supreme People's court may provide a judicial interpretation concerning issues on Article 43 of the E-commerce law, and adopting the blocking injunction is one of the feasible options to consider. If the Supreme People's court decides to adopt blocking injunction mechanism to solve online IP issues, Section 115A of the Australia Copyright Act provides a blocking injunction model as a reference.

---

565 RPRD, *supra* note 45, art. 22-25.
566 Tort Liability Law, *supra* note 51, art. 36.
567 2012 Provision, *supra* note 241, art 9.
568 E-commerce Law, *supra* note 25, art. 43.

In sum, the Internet policy of China shows a trend that both the Chinese legislation and government adopt an active-preventive approach to ISPs. Because the Chinese government adopted a strict policy to control its Internet environment, it is possible that China may adopt a government-supervised blocking injunction system to strengthen its IP protection against online piracy. After implementing a government-supervised blocking injunction system into administrative regulations for trial implementation, the Chinese legislation may consider establishing a court-supervised blocking injunction system and enact it into laws.

3. Summary

In conclusion, China should consider establishing a government-supervised blocking injunction system for the benefit of online copyright protection. To solve the issue of ISPs on copyright infringement, both the Chinese legislation and the people's courts adopted direct and secondary copyright liability theories of ISPs from the U.S., which shows the trend that China is shifting from a passive-reactive approach of ISPs toward an active-preventive approach of ISPs. After examining serval alternative solutions for the online copyright infringement issues of ISPs from different jurisdictions, this chapter concludes that an appropriate solution for China to strengthen online copyright protection is to establish a blocking injunction system based on current Internet policies and censorship systems. Although jurisdictions such as Australia established a court-supervised blocking injunction system, this chapter suggests that establishing a government-supervised blocking injunction system can be a more effective solution for China.

Chapter VI: Conclusion

After the comparison of ISPs related laws between the U.S. and China, this dissertation seeks to demonstrate that a traditional passive-reactive approach of ISPs is no longer able to effectively prevent IP infringements in the current Internet market. Therefore, some jurisdictions such as China is shifting from a passive-reactive model of ISPs to an active-preventive model of ISPs in order to protect IP more effectively. Before the E-commerce Law, although China followed a passive-reactive approach of ISPs, derived from the U.S., by enacting a DMCA-like system of ISPs in different laws and regulations, piracy and counterfeit perpetrated over the Internet continues to grow, and ISPs continue to be passive on IP protection. Therefore, the Chinese legislation adopted an active-preventive approach of ISPs in the E-commerce Law by establishing a unified IP protection system of ISPs.

The unified IP protection system of ISPs includes two parts. First, Article 41 to 45 of the E-commerce law establishes an active-preventive model of ISPs that compels ISPs to actively protect IP. Although giant ISPs such as Alibaba developed multiple proactive monitoring technical measures and cooperated with different stakeholders to prevent IP infringement,[569] the requirements of the E-commerce Law are comparatively lower: (1) ISPs shall establish a N&T system based on the principles from Article 42 to 45; (2) ISPs shall actively cooperate with IP holders to protect their IPRs.[570] However, compared to a passive-reactive approach of ISPs such as the DMCA, the E-commerce Law imposed more proactive obligations on ISPs.

Second, Article 5 of the E-commerce Law sets up a comprehensive mechanism of ISPs, which constitutes a blueprint for the Chinese legislation to improve IP protection system of ISPs in the future. For example, Article 5 of the E-commerce Law requires ISPs to follow the

[569] *See* Chapter IV Part III Section A.
[570] E-commerce Law, *supra* note 25, art. 41.

obligation in anti-unfair competition law, and the Chinese legislation enacted the Internet Clause in the 2017 Anti-unfair Competition Law to prevent the similar legal issues in *Tencent*. Therefore, Article 5 provides a legal foundation for Chinese legislation to improve mechanism of ISPs in different laws and regulations, including IP protection system.

In addition to the E-commerce Law, the Chinese legislation also adopted the active-preventive approach of ISPs in the Draft of the Third Amendment of the Copyright Law. Because Article 2 of the E-commerce Law excludes Internet Content Providers from the E-commerce Law, the Chinese legislation plans to enact relevant provisions in the Copyright Draft to avoid legal conflict. Notably, Although Article 73 of the Copyright Draft follows a passive-reactive approach of ISPs and provides safe harbor provisions for ISPs, Paragraph 5 Article 73 of the Copyright Draft particularly excludes the Internet Content Providers from the safe harbor provisions. In other words, the Internet Content Providers are not eligible for safe harbor, and therefore, has "a higher duty of care" to prevent copyright infringement. As a result, it is highly possible that the Chinese legislation may follow an active-preventive approach in the Third Amendment of the Copyright Law by imposing more duties of care on the Internet Content Providers.

Compared to a passive-reactive approach of ISPs, an active-preventive approach imposes more duties on ISPs. This might raise one further concern about the potential costs of this approach: innovative and start-up ISPs might be chilled by the burden of affirmative duties. However, due to the serious IP infringement issues in China, giant ISPs in China such as Alibaba adopted an active-preventive approach to promote IP protection. Notably, the achievement of Alibaba on IP protection in 2017 demonstrates that an active-preventive model can prevent IP infringement more effectively.[571] Nonetheless, merely one ISP is not able to solve the infringement issues because any infringers can easily switch from one ISP to another.

[571] See e.g. 2017 IP Report, *supra* note 452, at 4-6.

Therefore, it is necessary to establish a unified IP protection system and compel all ISPs to actively prevent IP infringements in China.

Although the E-commerce Law sets up the construction of a unified IP protection system of ISPs, this system is incomplete because the provisions merely provide general principles of an active-preventive model of ISPs. To improve this unified IP protection system of ISPs, this dissertation suggests that the Chinese legislation could legally transplant the blocking injunction system in ISPs related laws and regulations in order to protect IP more effectively. According to Article 6 and 7 of the E-commerce Law, because the Chinese government is authorized to supervise and govern e-commerce,[572] the administrative departments could establish a government-supervised blocking injunction system based on the Great Firewall system. Alternatively, the Chinese legislation can establish a court-supervised blocking injunction system based on Article 43 of the E-commerce Law. With the development of the IP Court and the Internet Court, Chinese legislation can follow the OADP of Australian Copyright Act and set up a court-supervised blocking injunction system for trial implementation in the future.

Once the Chinese legislation decides to establish a court-supervised blocking injunction system, this dissertation suggests that the Supreme People's Court could publish a judicial interpretation and grant jurisdiction to the Internet Court as the trial court for trial implementation. Based on the online features, the Internet Court can develop its online platforms to establish a court-supervised blocking injunction system for IP protection. If the disputes remain unsolved in the Internet Court, the IP Court shall have jurisdiction to hear the case as the higher-level court.

[572] E-commerce Law, *supra* note 25, art. 6-7.

Bibliography

Books

- CRAIG JOYCE ET AL., COPYRIGHT LAW (LexisNexis. 9th ed. 2013).
- GRAEME B. DINWOODIE, SECONDARY LIABILITY OF INTERNET SERVICE PROVIDERS (Graeme B. Dinwoodie ed., Springer 2017).
- JAANI RIORDAN, WEBSITE BLOCKING INJUNCTION UNDER UNITED KINGDOM AND EUROPEAN LAW (Graeme B. Dinwoodie ed., Springer 2017).
- JIE WANG, REGULATING HOSTING ISPS' RESPONSIBILITIES FOR COPYRIGHT INFRINGEMENT (Springer 2018).
- 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).
- PAUL GOLDSTEIN & MARKETA TRIMBLE, INTERNATIONAL INTELLECTUAL PROPERTY LAW CASES AND MATERIALS (Foundation Press, 4th ed. 2016).
- 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).
- SHANGHAI INTELLECTUAL PROPERTY COURT (上海知识产权法院), SHANGHAI INTELLECTUAL PROPERTY COURT JUDGMENTS SELECTION (2015-2016) [上海知识产权法院裁判文书精选 (2015-2016)] [Wang Qiuliang (王秋良) et al. eds., Global Tone Communication Technology (Shanghai) Co. Ltd. [中译语通信息科技(上海)有

限公司] trans. Intellectual Property Press (知识产权出版社) 2018].

- SONG, SEAGULL HAIYAN, NEW CHALLENGES OF CHINESE COPYRIGHT LAW IN THE DIGITAL AGE (Wolters Kluwer 2011).
- WANG QIAN (王迁), COPYRIGHT LAW (著作权法) [China Renmin University Press (中国人民大学出版社) 2015].
- WILLIAM PATRY, MORAL PANICS AND THE COPYRIGHT WARS (Oxford University Press, 1st ed. 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).
- Althaf Marsoof & Dr Aipana Roy, *The Blocking Injunction: A Comparative and Critical Review of the EU, Singaporean and Australian Regimes*, 38 EUR. INTELL. PROP. REV. 92 (Issue 2) (2016).
- Douglas Lichtman & William Landes, *Indirect Liability for Copyright Infringement: An Economic Perspective*, 16 HARV. J. L. & TECH. 395 (2003).
- Elizabeth K. Levin, *A Safe Harbor for Trademark: Reevaluating Secondary Trademark Liability after Tiffany v. eBay*, 24 BERKELEY TECH. L.J. 491 (2009).
- Gazette of the Supreme People's Court of the People's Republic of China
- Jeremy de Beer & Christopher D. Clemmer, *Global Trends in Online Copyright Enforcement: A Non-Neutral Role for Network Intermediaries?*, 49 JURIMETRICS J. 375 (2009).

- 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.
- Lin Chengduo(林承铎) & An Nita(安妮塔) *Application of Digital Copyright Laws in the Context of Safe Harbor Agreement and Red Flag Test* (数字版权语境下避风港规则与红旗原则的适用), Electronics Intellectual Property (电子知识产权), No. 7, 2016.
- 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.
- Mark A. Lemley, *Rationalizing Internet Safe Harbors*, 6 J. on TELECOMM. & HIGH TECH. L. 101 (2007)
- Peter K. Yu, *The Graduated Response*, 62 FLA. L. REV. 1373 (2010)
- Qin Han (秦汉), *Research on Dispute Resolution Mechanism of China's Internet Court* (互联网法院纠纷处理机制研究), Electronics Intellectual Property (电子知识产权), No. 10, 2018.
- Quan Yanmin (权彦敏), *The Analysis of Site-blocking Injunction to Reduce Online Copyright Infringement* (“封网禁令”探析), Electronics Intellectual Property (电子知识产权), No. 11, 2017.
- Ridwan Khan, *Pure Software in an Impure World? WINNY, Japan's First P2P Case* 8

E. ASIA L. REV. 21, 24 (2013)

- Shu Yihong (疏义红) & Xu Jisheng (徐记生), *From the Online Dispute Resolution to the Internet Court* (从在线争议解决到互联网法院), People's Court Daily (人民法院报), Nov. 11, 2017.
- Tian Xiaojun (田小军) & Zhu Yu (朱萸), *Comments on the Internet Clause of the Amendment of Anti-Unfair Competition Law of China* (新修订《反不正当竞争法"互联网专条" 评述), Electronics Intellectual Property (电子知识产权), No. 1, 2018.
- Wu Handong (吴汉东), *The Background, Layout and emphasis on the Third Amendment of the Copyright Law*, (《著作权法》第三次修改的背景、体例和重点), Law and Business Research (法商研究), issue 4, 2012.
- 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.
- Zhang Yong (张勇) & Wang Huayi (王铧翊), *On the Practical Challenges of the Adoption of Safe Harbor Rule in China* (论安全港规则在中国适用的现实挑战), Electronics Intellectual Property (电子知识产权), No. 1, 2018.
- Zuo Yuru (左玉茹), *Comments on the Draft of the Third Amendment of the Copyright Law* (《著作权法》第三次修改草案述评), Electronics Intellectual Property (电子知识产权), No. 4, 2012.

Cases

- American Broadcasting Crop. v. Aereo, 134 S. Ct. 2498 (2014).

- Bei jing qi hu ke ji you xian gong si, qi zhi ruan jian (bei jing) you xian gong si yu teng xun ke ji (shen zhen) you xian gong si, shen zhen shi teng xun ji suan ji xi tong you xian gong sib u zheng dang jing zhen jiu feng an er shen min shi pan jue shu [北京奇虎科技有限公司、奇智软件（北京）有限公司与腾讯科技（深圳）有限公司、深圳市腾讯计算机系统有限公司不正当竞争纠纷案二审民事判决书 [Qihoo Tech Ltd. (Beijing) v. Tencent Tech Ltd. (Shenzhen)], [Sup. People's Ct. (中华人民共和国最高人民法院) Feb 18, 2014], (2013) Min San Zhong Zi No. 5 [(2013) 民三终字第5号] (China).
- Bei jing Zhong qiang wen wen hua chuan mei you xian gong si deng zhu zuo quan quan shu, qing quan jiu fen ger shen ming shi pan jue shu (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) [Beijing China Youth Publishing Group v. Beijing Baidu Tech. Ltd.], [Beijing High People's Ct. (北京市高级人民法院) Aug 5, 2014], 2014 Gao Min Zhong Zi No. 2045 [(2014) 高民终字第2045号)](China).
- Yi nian (shang hai) shi zhuang mao yi you xian gong si su zhe jiang tao bao wang luo you xian gong si, du guo fa qing hai shang biao quan jiu fen [衣念（上海）时装贸易有限公司诉浙江淘宝网络有限公司、杜国发侵害商标权纠纷] [E. LAND Ltd. (Shanghai) v. Zhejiang Taobao Network Ltd.], [Shanghai First Interm. People's Ct. (上海市第一中级人民法院)] [(2011) Hu Yi Zhong Min Wu (Zhi) Zhong Zi No. 40 (沪一中民五(知)终字第40号)] (China).
- *Fonovisa, Inc. v. Cherry Auction, Inc.,* 76 F.3d 259 (9th Cir. 1996)
- Fei hu xin xi ji shu (tian jin) you xian gong si su shang hai huan dian xin xi ke ji you xian gong si qin hai zuo pin xin xi wang luo chuan bo quan jiu fen shang su an [飞狐

信息技术(天津)有限公司诉上海幻电信息科技有限公司侵害作品信息网络传播权纠纷上诉案] [*TV.SOHO.COM (Tianjin) v. Shanghai Hode Information Technology Co. Ltd.*], Shanghai IP Ct. (上海知识产权法院) Mar 25, 2016] (2015) Hu Zhi Min Zhong Zi No. 276 [(2015)沪知民终字第276号](China).

- *Gershwin Publishing Corp. v. Columbia Artists Management, Inc.,* 443 F.2d 1159 (2d Cir.1971)
- *Inwood Laboratories, Inc. v. Ives Laboratories, Inc.,* 456 U.S. 844 (1982).
- *MDY Industries, LLC. v. Blizzard Entertainment, Inc.*, 629 F.3d 928 (2011).
- *Metro-Goldwyn-Mayer Studios Inc. v. Grokster, Ltd.* 125 S. Ct. 2764 (2005)
- *Music Copyrght Society of China (MCSC) v. Guangzhou NetEase Inc. and China Mobile Beijing Ltd.*, Beijing Second Intermediate People's Ct. (2002) Er Zhong Min Chu Zi No. 03119.
- *Parker v. Google, Inc.*, 242 Fed.Appx. 833 (3d Cir.2007)
- *Roadshow Films Pty Ltd v. Telstra Corporation Ltd* [2016] FCA 1503 (Austl.)
- Shang hai ju li chuan mei ji shu you xian gong si su shang hai da mo wang luo ke ji you xian gong si qi ta bu zheng dang jing zhen jiu fen shang su an (上海聚力传媒技术有限公司诉上海大摩网络科技有限公司其他不正当竞争纠纷上诉案) [*Shanghai Synacast Media Technology Co., Ltd. v. Shanghai Damo Network Technology Co., Ltd.*], Shanghai IP Ct. (上海知识产权法院) Jul 15, 2016, (2016) Hu No. 73 Min Zhong No. 34 [(2016) 沪73民终34号] (China).
- *Sony Corp. of America v. Universal City Studios, Inc.,* 104 S.Ct. 774, 785 (1984)
- *Tiffany (NJ) Inc. v. eBay Inc.*, 600 F.3d 93 (2d Cir. 2010).
- *Twentieth Century Fox Film Corp. v. British Telecommunications plc* [2011] EWHC 1981 (Ch).

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

Statutes

- 15 U.S.C.§1127 (2000)
- 17 U.S.C.§101 (2010)
- 17 U.S.C.§106 (2002)
- 18 U.S.C.§2510 (2002)
- Communications Decency Act, 47 U.S.C.§230 (1996)
- WIPO Copyright Treaty Art 8.
- Digital Millennium Copyright Act, 17 U.S.C.§512 (2010)
- Copyright Designs and Patent Act 1988 (UK)
- Telecommunications Act 1997 (Australia)
- Copyright Act 1968 (Australia)
- 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 on the Protection of the Right of Dissemination via Information Network] (promulgated by the St. Council, May 18, 2006, amended by the St. Council in Jan 30, 2013). The English translation is available at http://www.cpahkltd.com/UploadFiles/20100315165559735.pdf. (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) (China). Translated by Westlawchina (www.westlawchina.cn).
- Zhong hua ren min gong he guo dian zi shang wu fa (中华人民共和国电子商务法) [E-commerce Law of People's Republic of China] (promulgated by the Standing Comm. Nat'l People's Cong., Aug 31, 2018, effective Jan 1, 2019) (China). Translated by Westlawchina (www.westlawchina.cn).
- 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) (China). Translated by Bei da fa bao (北大法宝) (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 Liability Law of the PRC] (promulgated by the Standing Comm. Nat'l People's Cong., Dec. 26, 2009, effective in Jul. 1, 2010) (China). Translated by Westlawchina (www.westlawchina.cn)
- Zhong hua ren min gong he guo jing cha fa (中华人民共和国警察法) [People's Police Law of the PRC] (promulgated by the Standing Comm. Nat'l People's Cong.,

Feb. 28, 1995, amended by the Standing Comm. Nat'l People's Cong., Oct. 26, 2012, effective in Jan. 1, 2013) (China). Translated by Westlawchina (www.westlawchina.cn)

- Zhōnghuá rénmín gònghéguó rénmín 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 PRC] (promulgated by the St. Council, Jul 1, 1979, amended by the St. Council in Oct 26, 2018, effective in Jan 1, 2019) (China). Translated by Westlawchina (www.westlawchina.cn).
- Zhong hua ren min gong he guo shang biao fa (中华人民共和国商标法) [Trademark Law of the PRC] (first promulgated by the Standing Comm. Nat'l People's Cong., Fed. 22, 1993, amended by the Standing Comm. Nat'l People's Cong. in Aug. 30, 2013, effective in May 1, 2014) (China). Translated by Westlawchina (www.westlawchina.cn).
- Zhong hua ren min gong he guo shang biao fa shi shi tiao li (中华人民共和国商标法实施条例) [Implementing Regulations of the Trademark Law of the PRC] (promulgated by the St. Council, Apr. 29, 2014, effective in May 1, 2014) (China). Translated by WestlawChina (www.westlawchina.cn).
- LOI no 2009-669 du 12 juin 2009 favorisant la diffusion et la protection de la cr6ation 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 Rdpublique Frangaise [J.0.] [Official Gazette of France], June 12, 2009, p. 9666, (France)
- Fan bu zheng dang jing zheng fa (反不正当竞争法), Anti-unfair Competition Law of the PRC, promulgated by the Standing Comm. Nat'l People's Cong., Sep. 2, 1993, effective in Dec. 1, 1993 (China). Translated by Westlawchina

(www.westlawchina.cn).

- Fan bu zheng dang jing zheng fa (反不正当竞争法), Anti-unfair Competition Law of the PRC, promulgated by the Standing Comm. Nat'l People's Cong., Nov 4, 2017, effective Jun 1, 2018 (China). Translated by Westlawchina (www.westlawchina.cn).
- Zhong hua ren min gong he guo wang luo an quan fa (中华人民共和国网络安全法) [Network Security Law of People's Republic of China] (promulgated by the Standing Comm. Nat'l People's Cong., Nov 7, 2016, effective Jun 1, 2017. (China). Translated by Westlawchina (www.westlawchina.cn).
- Zhong hua ren min gong he guo ji suan ji xin xi an quan bao hu tiao li (中华人民共和国计算机信息安全保护条例) [Regulations of the People's Republic of China for Safety Protection of Computer Information Systems] (promulgated by the State Council, effective in Feb. 18, 1994, amended by the State Council, Jan. 8, 2011, Feb. 18, 1994) (China). Translated by Westlawchina (www.westlawchina.cn).
- Hu lian wang fu wu guan li ban fa (互联网服务管理办法) [Measures on Internet Information Services] (promulgated by the State Council, Sep. 25, 2000, amended by the State Council, Jan. 8, 2011, effective in Sep. 25, 2000) (China). Translated by Westlawchina (www.westlawchina.cn).

Legislative materials

- S. REP. No. 105-190 (1998).
- H.R. REP. 105-551(II) (1998).
- Explanatory Memorandum, Copyright Amendment (Online Infringement) Bill 2015 (Cth) (Australia)
- Zhong hua ren min gong he guo zhu zuo quan fa (xiu ding fa an song sheng gao) [中

华人民共和国著作权法(修订草案送审稿)] [Draft of the Copyright Law of the PRC (2014)] (published by the Legislative Affairs Office of the State Council of the PRC). Available at https://npcobserver.files.wordpress.com/2017/08/copyright-law-2014-draft-revision.pdf.

- Zhong hua ren min gong he guo dian zi shang wu fa (cao an) [中华人民共和国电子商务法(草案)] [First Draft of the E-commerce Law (Dec 2016)] (published by the Standing Comm. Nat'l People's Cong. in Dec. 2016), available at https://npcobserver.files.wordpress.com/2016/12/e-commerce.pdf.
- Zhong hua ren min gong he guo dian zi shang wu fa (er ci sheng yi gao) [中华人民共和国电子商务法(二次审议稿)] [Second Deliberation Draft of the E-commerce Law (Oct 2017)] (published by the Standing Comm. Nat'l People's Cong. in Oct. 2017), available at https://npcobserver.files.wordpress.com/2017/11/e-commerce-law-2nd-draft.pdf.
- Zhong hua ren min gong he guo dian zi shang wu fa (san ci sheng yi gao) [中华人民共和国电子商务法(三次审议稿)] [Third Deliberation Draft of the E-commerce Law (Jan 2018)] (published by the Standing Comm. Nat'l People's Cong. in Jan 2018), available at https://npcobserver.files.wordpress.com/2018/06/e-commerce-law-3rd-draft.pdf.
- NPC Law Committee (全国人民代表大会法律委员会), Report of the NPC Law Committee to amend the Draft of the E-commerce Law of the PRC (全国人民代表大会法律委员会关于《中华人民共和国电子商务法(草案)》修改情况的汇告), Oct 31, 2017. Available at: http://www.npc.gov.cn/npc/xinwen/2018-08/31/content_2060144.htm.
- NPC Constitution and Law Committees (全国人民代表大会宪法和法律委员会),

Report of the NPC Constitution and Law Committees to amend the Draft of the E-commerce Law of the PRC (全国人民代表大会宪法和法律委员会关于《中华人民共和国电子商务法(草案)》修改情况的汇告), Jun 19, 2018. Available at: http://www.npc.gov.cn/npc/xinwen/2018-08/31/content_2060320.htm

Judicial materials

- Hangzhou Court of the Internet (杭州互联网法院), The Trial Procedure of the Litigation Platform of Hangzhou Internet Court (杭州互联网法院网上庭审规范). Available at https://www.netcourt.gov.cn/portal/main/domain/lassen.htm?lang=En#lassen/litigationDocuments (last visited Nov. 25, 2018).
- Hangzhou Internet Court (杭州互联网法院), Hangzhou Internet Court's Guidelines Regarding the Litigation and Jurisdiction of the Internet-involved Cases (杭州互联网法院案件管辖指引). Available at https://www.netcourt.gov.cn/portal/main/domain/lassen.htm?lang=En#lassen/litigationDocuments (last visited Nov. 25, 2018).
- Hangzhou Internet Court (杭州互联网法院), Provisions on the Electronic Evidence platform of the Hangzhou Internet Court (Trial Implementation) [杭州互联网法院电子证据平台规范(试行)]. Available at https://www.netcourt.gov.cn/portal/main/domain/lassen.htm?lang=En#lassen/litigationDocuments (last visited Nov. 25, 2018).
- www.netcourt.gov.cn(杭州互联网法院诉讼平台), English vision is available at http://www.netcourt.gov.cn/portal/main/domain/index.htm?lang=En.
- Hangzhou Court of the Internet (杭州互联网法院), Rule on Asynchronous Trial

related to Internet cases (trial implementation) [涉网案件异步审理规程(试行)]. Available at https://www.netcourt.gov.cn/portal/main/domain/lassen.htm#lassen/litigationDocuments.

- 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 via 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. (China). Translated by Bei da fa bao (北大法宝) (en.pkulaw.cn).
- Zui gao ren min fa yuan guan yu zhi shi chan quan fa ting ruo gan wen ti de gui ding (最高人民法院关于知识产权法庭若干问题的规定) [Provisions of the Supreme People's Court on Several Issues Concerning Intellectual Property Tribunal] (promulgated by the Supreme People's Court, Dec. 3, 2018, effective in Jan. 1, 2019) (China), art. 1.
- Zui gao ren min fa yuan guan yu hu lian wang fa yuan shen li an jian ruo gan wen ti de gui ding (最高人民法院关于互联网法院审理案件若干问题的规定) [Provisions of the Supreme People's Court on Several Issues Concerning Trial of Cases by the Internet Courts] (promulgated by the Supreme People's Court, Sep. 6, 2018, effective in Sep. 7, 2018) (China) Fa Shi (2018) No. 16 [法释(2018)16号]. Translated by Westlawchina (www.westlawchina.cn).
- Zui gao ren min fa yuan guan yu Beijing Shanghai Guangzhou zhi shi chan quan fa

yuan shen an jian guang xia de gui ding (最高人民法院关于北京、上海、广州知识产权法院案件管辖的规定) [Provisions of the Supreme People's Court on the Jurisdictions over Cases by Intellectual Property Courts in Beijing, Shanghai and Guangzhou] (promulgated by the Supreme People's Court, Oct. 31, 2014, effective in Nov. 1, 2014) (China) Fa Shi No. 12 (2014) [法释(2014) 12号]. Translated by Westlawchina (www.westlawchina.cn).

- Notice of the Supreme People's Court on Issuing the Plan for Adding the Beijing Internet Court and the Guangzhou Internet Court (最高人民法院印发《关于增设北京互联网法院、广州互联网法院的方案》的通知) No. 216 (2018) [法(2018)216号].
- Zui gao ren min fa yuan guan yu sheng li zhu zuo 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著作权民事纠纷案件适用法律若干问题的解释) [Interpretation of the Supreme People's Court on Certain Issues Concerning the Application of Law in the Trial of Civil Cases Involving Copyright Disputes] (promulgated by the Sup. People's Ct., Oct. 12, 2002, effective Oct. 15, 2002) Interpretation No. 31 (2012) [法释(2012)20号] (China). Translated by Westlawchina (www.westlawchina.cn).
- Zu gao ren min fa yuan guan yu an li zhi dao gong zuo de gui ding (最高人民法院关于案例指导工作的规定) [Provisions of the Supreme People's Court on Case Guidance Work] (promulgated by the Sup. People's Ct., Nov. 26, 2010, effective Nov. 26, 2010) (China) Fa Fa No. 51 (2010) [法发(2010) 51号]. Translated by Westlawchina (www.westlawchina.cn).

Internet Materials

- 2016 Intellectual Property Rights Protection in China, http://english.sipo.gov.cn/docs/2018-01/20180131135159213892.pdf (last visited Aug. 28, 2018).
- 2017 Situation Report on Counterfeiting and Piracy in the European Union https://www.europol.europa.eu/publications-documents/2017-situation-report-counterfeiting-and-piracy-in-european-union (last visited Aug. 24, 2018).
- 41st Statistical Report on Internet Development in China, http://cnnic.cn/hlwfzyj/hlwxzbg/hlwtjbg/201803/P020180305409870339136.pdf (last visited Sep 8th, 2018). English version is available at http://cnnic.com.cn/IDR/ReportDownloads/201807/P020180711391069195909.pdf.
- Alibaba Group, *IPP Platform Principle & Policy*, Available at https://ipp.alibabagroup.com/policy/en.htm (last visited Oct. 19, 2018).
- Alibaba Group, *Alibaba Group 2017 Intellectual Property Rights Protection Annual Report*, Available at http://azcms31.alizila.com/wp-content/uploads/2018/05/Alibaba-Group-PG-Annual-Report-2017-FINAL_sm_final.pdf (last visited Oct. 20, 2018).
- Althaf Marsoof, *The Blocking Injunction – A Critical Review of Its Implementation in the United Kingdom Within the Legal Framework of the European Union*, http://crossmark.crossref.org/dialog/?doi=10.1007/s40319-015-0379-z&domain=pdf (last visited Aug. 25, 2018).
- ALIBABA PUBLIC JURY, HTTPS://PAN.TAOBAO.COM (LAST VISITED DEC. 25, 2018).
- BBC, *Fortnite cheat YouTuber sued by Epic Games*, Available at https://www.bbc.com/news/technology-45876864 (last visited Oct. 18, 2018).
- The State Council Information Office of the People's Republic of China (中华人民共和国国务院新闻办公室), China and World Trade Organization (《中国与世界贸易组织》白皮书). Available at

http://www.scio.gov.cn/zfbps/32832/Document/1632334/1632334.htm (last visited Aug. 9th, 2018). English version is available at http://www.scio.gov.cn/zfbps/32832/Document/1632345/1632345.htm.

- Indiana University, Copyright infringement incident resolution, https://protect.iu.edu/online-safety/personal-preparedness/file-sharing/violations.html (last visited Oct. 25, 2016).
- Indiana University, Copyright tutorial, https://protect.iu.edu/online-safety/personal-preparedness/file-sharing/tutorial.html (last visited Oct. 25, 2016).
- Chris Hoffman, *How the "Great Firewall of China" Works to Censor China's Internet*, Howtogeek (Sep. 22, 2016), https://www.howtogeek.com/162092/htg-explains-how-the-great-firewall-of-china-works/ (last visited Nov. 24, 2018).
- Du Mingming, Bianji, Chinese copyright regulator publicizes piracy cases, Xinhua (新华网) (Apr. 27, 2017, 09:07), http://en.people.cn/n3/2017/0427/c90000-9208308.html (last visited Aug. 22, 2018).
- 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)
- Hangzhou Court of the Internet, Network Copyright Judicial Protection Report (April 2018), http://hztl.zjcourt.cn/ (last visited Nov. 3, 2018)
- Heather Kelly, Google's CEO says it's still considering a censored search engine in China, CNN (Oct. 16, 2018 12:14 A.M.) https://www.cnn.com/2018/10/15/tech/google-china-sundar-pichai/index.html. (last visited Nov. 24, 2018)
- 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)

- James Griffiths, *China is exporting the Great Firewall as internet freedom declines around the world*, CNN (Nov. 2, 2018 2:00 A.M.) https://www.cnn.com/2018/11/01/asia/internet-freedom-china-censorship-intl/index.html (last visited Nov. 23, 2018)
- Jiang Jie, *China highlights IPR protection to encourage creativity*, People's Daily Online (人民网), (12:03, Aug. 23, 2018) available at http://en.people.cn/n3/2018/0823/c90000-9493519.html (last visited Oct. 23, 2018)
- Liang Jun & Bianji, *China probes online group discounter Pinduoduo over counterfeit allegation*, Xinhua (新华网) (Aug. 2, 2018, 08:29), http://en.people.cn/n3/2018/0802/c90000-9486961.html (last visited Aug. 23, 2018).
- Liang Jun & Bianji, *Pinduoduo told to fix fake goods issue*, China Daily (Aug. 4, 2018, 11:36), http://en.people.cn/n3/2018/0804/c90000-9487727.html (last visited Aug. 24, 2018).
- 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).
- National Copyright Administration of the PRC (中华人民共和国国家版权局), Report of the "Sword Net Campaign 2017," ("剑网 2017"专项行动的有关通报) Jan 16, 2018. Available at http://www.ncac.gov.cn/chinacopyright/contents/10873/357502.html.
- NETFLIX, *How does Netflix work?* https://help.netflix.com/en/node/412?lang=en&nodeId=412 (last visited Aug. 27, 2016)

- NPC Standing Committee (全国人大常委会), Press conference of the General Office of the NPC Standing Committee (2018.08.31) (全国人大常委会办公厅2018年8月31日新闻发布会). Available at http://www.npc.gov.cn/npc/zhibo/zzzb36/node_27366.htm (last visited Sep. 23, 2018).
- 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).
- Office of the United States Trade Representative, 2017 Special 301 Report, available at https://ustr.gov/sites/default/files/301/2017%20Special%20301%20Report%20FINAL.PDF.
- www.gov.cn (中华人民共和国中央人民政府), *China's focus on Internet Plus governance*, (Feb. 1, 2017, 09:17 AM). Available at: http://english.gov.cn/premier/news/2017/02/01/content_281475556331388.htm (last visited Nov. 18, 2018).
- www.gov.cn (中华人民共和国中央人民政府), *Measures taken to promote Internet Plus government service*, (Aug. 18, 2017, 02:13 PM). Available at: http://english.gov.cn/premier/news/2017/08/18/content_281475798536474.htm (last visited Nov. 18, 2018).
- Xiao Qiang, How China's Internet Police Control Speech on the Internet, (Nov. 24, 2008) Radio Free China. Available at https://www.rfa.org/english/commentaries/china_internet-11242008134108.html (last

visited Sep. 23, 2018).

- Xinhua (新华网), China to launch Internet courts in Beijing, Guangzhou, (07:53, July 26, 2018), available at http://en.people.cn/n3/2018/0726/c90000-9484769.html (last visited Nov. 23, 2018).
- Yan, China Focus: China adopts e-commerce law to improve market regulation, Xinhau, (Aug. 31, 2018 23:07). Available at: http://www.xinhuanet.com/english/2018-08/31/c_137434452.htm (last visited Sep. 23, 2018).
- Zhang Yanlai, Rise of Internet Court, Zhihe college, https://mp.weixin.qq.com/s/zCIPRzBReW5W_XULb-UFIA (last visited Aug. 23, 2018).

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).