Article

# Establishing Certainty of Internet Service Provider Liability and Safe Harbor Regulation

**Jerry Jie Hua** *

ABSTRACT

*In response to the conventional requirement of protecting the right of communication to the public and the widespread online copyright piracy, copyright laws and policies among different jurisdictions extend infringing liability to internet service providers (ISPs) which induce or facilitate their subscribers' infringing activities. Although safe harbor has been developed from judicial practices and been incorporated into legislations, proceedings such as notice and takedown, subpoena procedure and the graduated response policy would still suffocate information dissemination and infringe individual privacy.*

*This paper intends to provide proposals for setting up certainty of ISP liability and alleviating current tendency to aggravate ISP liability in general, and recommend suggestions for China's digital copyright reform on ISP liability by reviewing and analyzing existing copyright systems regarding ISP liability among different jurisdictions. The second part will examine the definition of ISP and the importance of establishing certainty and predictability of indirect liability. The third part will analyze the safe harbor rule and contributory and vicarious liability developed through American court judgments, as well as the authorization and joint*

DOI：10.3966/181263242014030901001

* Associate (Legal Assistant title) at Deacons (Hong Kong); PhD (Intellectual Property Law), The University of Hong Kong; LLM in Comparative Law, University of Florida; LLB, China Foreign Affairs University. E-mail: jerryhua@connect.hku.hk. This article is based on chapters in the PhD thesis titled "Toward A More Balanced Approach: Rethinking and Readjusting Copyright Systems in the Digital Network Era" submitted to The University of Hong Kong for partial fulfillment of the PhD degree. The author wishes to thank The University of Hong Kong for its Graduate Studentship in financial support of the research.

*tortfeasor liability developed from cases in Commonwealth jurisdictions. The fourth part will examine the statutory requirements regarding ISP liability and its limitation. The statutes reviewed in this part will be mainly from the United States, China, and Hong Kong, as the combination of statutory regulations in these jurisdictions represents a relatively complete regime for ISP liability. The fifth part will examine the "graduated response" policy, the new development on aggravating ISP liability through adding new conditions for safe harbor in some jurisdictions such as France. The sixth part will suggest proposals for adjusting current digital copyright laws on ISP liability in general and China's digital copyright reform in particular so as to balance the interests among copyright owners, intermediaries such as ISPs and internet users and establish certainty for ISP liability.*

***Keywords:*** *Internet Service Providers (ISPs), Indirect Infringing Liability, Safe Harbor, Balance of Interest*

CONTENTS

## I. INTRODUCTION

Copyright works are often distributed through technological and media intermediaries. Books are commonly available to public readers because of the invention of the printing press and the establishment of publishing companies. Songs, TV programs and movies are available to a large number of listeners and viewers because of the birth of sound recorders, radios, televisions, satellites and movie theatres. The development of computers and digital technology and the emergence of the internet in the late twentieth century have greatly changed how people are accessing and distributing copyright works. In the digital network world, anyone who has access to a computer and the internet can easily make multiple perfect copies of the original copyright work in very little time and distribute either the original work or the copies by uploading them onto a website or emailing them as attachments to friends. Moreover, skilled digital technology users can easily revise, modify and adapt copyright works by using different technological tools. When connected via the digital network, either the original or the derivative work can easily be found due to the strong searching and linking capabilities of internet resources. Peer-to-peer file sharing technology and portable electronic devices, such as MP3s and iPods, have further increased the reproduction and distribution of copyright works. These new technologies allow users to make works available to the public as they please. Intermediaries themselves do not distribute copyright works.

Prior to the emergence of digital network technology, it was possible for copyright owners to find and track copyright infringers as well as address piracy either through administrative or judicial procedures, because infringers in the pre-internet world needed time and effort to produce pirated copies and find appropriate channels to sell them. They are companies or individuals whose identity can be confirmed. Due to the human and financial resources necessary for the production of counterfeit goods, the number of copyright infringers was not that large compared to the number of legal consumers of copyright works. In contrast, with the facilitation of digital network technology, any internet surfer can easily infringe copyright works by simply clicking the computer mouse and uploading or downloading copyright works, as long as their activities are not authorized by the relevant copyright owners. Peer-to-peer file sharing technology can allow thousands of copyright works to be uploaded and downloaded simultaneously. Therefore, it would not be that convenient or easy for copyright owners to sanction and sue every individual infringer. Looking for every copyright infringer is not only costly and time-consuming, but under certain situations, it is impossible for copyright owners to confirm the true identity of the infringer because of anonymity in the virtual world. In order to safeguard

their rights and interests, copyright owners, especially the powerful copyright industries, have begun to take action against intermediaries, mostly the ISPs that provide technologies and devices which facilitate infringement activity. They not only seek for judicial judgments that favor their standpoint, but also continuously lobby legislature to enact new laws that regulate the infringing liability of intermediaries.

The United States is one such a country that reflects the continuing battle of copyright owners against the intermediaries. It established the indirect infringing liability of ISPs through a few influential cases and enacted the Digital Millennium Copyright Act (DMCA) which contains a particular section on ISP liability related to material online. The indirect liability model of the United States has influenced many jurisdictions including China through legal transplant or bilateral free trade agreements. China enacted the Regulation on the Protection of the Right to Network Dissemination of Information in 2006 (thereafter, the 2006 Regulation) by following the United States legislative model to regulate the infringing liability of ISPs and adding provisions specific to the Chinese legal and social environment. The enactment of the regulation indirectly reflects the rapid increase of internet use in China and the necessity of establishing the liability of Chinese ISPs.

After connection to the internet was made possible in 1994, internet use in China has quickly spread year by year. According to the Statistical Survey Report on Internet Development in China issued by the China Internet Network Information Center (CNNIC) each year, the number of internet users in 2000 was 22.5 million and grew to 111 million in 2005.[1] The increase in the number of internet users remained robust in the following years. By June of 2011, the total number of internet users reached 485 million people and the penetration rate was 36.2%.[2] Entertainment and enjoyment of copyright contents remain a most important use of the internet. The number of subscribers of online music reached 382 million with a subscription rate of 78.7%.[3] The number of online video subscribers reached 301 million with a subscription rate of 62.1%.[4] These statistics demonstrate

1. *Semiannual Survey Report on Development of China's Internet*, CHINA INTERNET NETWORK INFORMATION CENTER (Jan., 2001), http://www.cnnic.net.cn/download/manual/en-reports/7.pdf; *17th Statistical Survey Report on the Internet Development in China*, CHINA INTERNET NETWORK INFORMATION CENTER (Jan., 2006), http://www.cnic.cas.cn/qkbg/cnnictjbg/cnnictjfz/200601/P020090819615860278077.pdf.

2. *28th Statistical Survey Report on the Internet Development in China*, CHINA INTERNET NETWORK INFORMATION CENTER (July, 2011), http://www1.cnnic.cn/IDR/ReportDownloads/201209/P020120904421102801754.pdf.

3. *Id.*

4. *Statistical Report on Internet Development in China*, CHINA INTERNET NETWORK INFORMATION CENTER (July, 2011), http://www1.cnnic.cn/IDR/ReportDownloads/201209/P020120904421102801754.pdf.

the necessity and importance of establishing certainty and predictability about the liability for ISPs and amending this liability to balance the interests of copyright owners and internet users. On the one hand, lack of invigilation and legal regulation of ISP liability will induce flooding of piracy online. On the other hand, enforcing overly strict liability for ISPs will suffocate data transmission and information dissemination, thus intervening with the enjoyment of copyright contents by internet users.

This article intends to provide proposals to establish certainty about liability for ISPs and alleviating current tendencies to aggravate ISP liability in general and recommend suggestions for China's digital copyright reform on ISP liability by reviewing and analyzing existing copyright systems in terms of ISP liability among different jurisdictions. The second part of the article will examine the definition of ISPs and the importance of establishing certainty and predictability about indirect liability. The third part will analyze the safe harbor system and contributory and vicarious liability developed through American court judgments. Certain elements in contributory and vicarious liability will be examined in detail, as these elements have been incorporated into digital copyright statutes. This part will also briefly analyze the authorization and joint tortfeasor liability developed from cases in Commonwealth jurisdictions, such as Australia and the United Kingdom, which will be compared with contributory and vicarious liability so as to conclude the consistent disciplines that are adopted to regulate ISP liability. After reviewing the rules and laws developed from common law cases, the fourth part of the article will examine the statutory requirements with respect to ISP liability and its limitations. The statutes will be mainly from the United States, China, and Hong Kong, as the combination of statutory regulations in these jurisdictions represents a relatively complete regime for ISP liability. The fifth part will examine the "graduated response" policy, the new development on aggravating ISP liability by adding new conditions for safe harbors in some jurisdictions, such as France. This part will argue against this new policy, as it will bring about more negative influence on information dissemination and freedom of expression than its positive impact on piracy control. The final part of the article will provide suggestions for proposals to amend current digital copyright laws on ISP liability in general and China's digital copyright reform in particular so as to balance the interests of copyright owners, intermediaries such as ISPs and internet users, and establish certainty about liability for ISPs.

## II. INTRODUCTION ON INTERNET SERVICE PROVIDERS

### A. *Definition of Internet Service Providers*

The first international copyright conventions that dealt with copyright challenges brought on by digital network technology are the WIPO Internet Treaties. However, these treaties do not include specific ISP liability regulations and leave room for member states to decide. Despite room to decide as pertaining to ISP liability, the WIPO Copyright Treaty (WCT) grants copyright owners the right of communication to the public by wire or wireless means so that "members of the public may access the works from a place and at a time individually chosen by them".[5] This provision confirms the right of control by copyright owners over the distribution of their works under a digital network environment. Any activity that allows the copyright contents to be made available to the public without authorization by the copyright owners constitutes infringement. However, in order to avoid the overexpansion of exclusive rights enjoyed by copyright owners, and to promote the development of technology, the Concerning Article 8 in the Agreed Statements Concerning the WCT particularly precludes the "provision of physical facilities for enabling or making a communication"[6] as exercise of the right of communication to the public within the meaning from the WCT or the Berne Convention for the Protection of Literary and Artistic Works. Such a provision indirectly provides safe harbors for technological intermediaries.

Among the member states of the WIPO Internet Treaties, the United States is the earliest country which enacted new copyright statutes to specifically deal with digital network challenges. Among the five titles of the DMCA, Title II, the "Online Copyright Infringement Liability Limitation Act", specifically addresses the issue of ISP liability and creates limitations on infringing liability for certain types of activities by ISPs. Title II of the DMCA has been incorporated into the United States Copyright Act as Section 512, titled "Limitations on Liability Relating to Material Online". Under the definition of Section 512, the term "service provider" means "a provider of online services or network access, or the operator of facilities therefor".[7] However, there is no further definition of "online services". Thus, this definition of a "service provider" is vague. There are two possible explanations. The first explanation is that the term "online services" could mean any service offered online, including making copyrighted contents

5. WIPO Copyright Treaty, art. 8, Dec. 20, 1996, 2186 U.N.T.S. 121.

6. *Agreed Statements Concerning the WIPO Copyright Treaty*, concerning art. 8, WIPO, http://www.wipo.int/treaties/en/text.jsp?file_id=295456.

7. 17 U.S.C. § 512(k)(1)(B) (2010).

available to the public.[8] Under this interpretation, anyone who operates a website could be an ISP. The second explanation is that the term should only mean services specific to being online.[9] Under this interpretation, only companies who host websites are ISPs; those who provide contents are not, as making contents available to the public is not internet-specific. One can provide copyrighted works through various channels such as paper publications, radio or television broadcasting, and online video broadcasting. Internet is one of the many media forms that can publish works, but not the sole medium.

Many defendants in ISP liability cases fall under the second definition. Both in the influential case *Sony Corp. v. Universal City Studios Inc.* and later cases that involved peer-to-peer file sharing technology, defendants who were deemed as ISPs merely supplied consumers with the tools and technology to facilitate reproduction and distribution of copyright works. The copyright contents were provided by third parties, such as TV program companies or internet subscribers. In a Chinese nation-wide influential case, *Music Copyright Society of China (MCSC) v. NetEase Inc. and China Mobile Beijing Ltd.,* trialed by the Beijing Second Intermediate People's Court in 2002,[10] the first defendant NetEase was sued for providing the music works of MCSC on its website for mobile phone users to download as phone ringtones. The second defendant, China Mobile Beijing, was sued for facilitating downloading by mobile phone users. The final judgment ruled against NetEase and for China Mobile Beijing primarily based on the reason that China Mobile could not select, modify or delete the transmitted information. As the first case in which an infrastructure service provider acted as co-defendant in an online copyright infringement issue, Chinese copyright law academia and practitioners consequently paid close attention. Judge Zhou Xiaobin of the Beijing Second Intermediate People's Court drew the conclusion from this case that internet infrastructure service providers could be divided into three major categories, that is, internet content provider (ICP), internet service provider (ISP) and internet apparatus provider (IAP). ICPs select, edit and upload information contents; ISPs facilitate the transmission of information without selecting or editing the contents; and IAPs provide essential apparatuses for network operation. The academic classification of service providers influenced by the Chinese court judgment also demonstrates that ISPs are mostly referred to website operators who

8. Jane C. Ginsburg, *User-Generated Content Sites and Section 512 of the US Copyright Act*, *in* COPYRIGHT ENFORCEMENT AND THE INTERNET 183, 187 (Irini A. Stamatoudi ed., 2010).

9. *Id.*

10. Chung Kuo Yin Lê Chao Tso Ch'üan Hsieh Hui v. Wang I Kung Ssu & I Tung T'ung Shên Kung Ssu [Music Copyright Society of China (MCSC) v. Guangzhou NetEase Computer System Inc. & China Mobile Beijing Co., Ltd.] (Beijing 2d. Interm. People's Ct. Sept. 20, 2002) (Westlaw China).

help transmit information rather than provide the contents.

Besides the statutory definition of ISPs and indication from the judgments, Section 512 of the DMCA also lists four categories of ISP conducts under which ISPs can be protected from copyright infringement liability subject to certain conditions. The four categories of ISP conducts are (1) "transitory digital network communications" which limit the liability of ISPs in circumstances where the provider merely acts as a data conduit, transmitting digital information from one point on a network to another at someone else's request; (2) "system caching" which limits the liability of ISPs that temporarily store the transmitted material made available online by a person other than the ISPs and deliver the material to the expected subscriber; (3) "storage of information on systems or networks at direction of users" which limits the liability of ISPs for infringing material on websites hosted on their systems; and (4) "information location tools" which limit the liability of ISPs that link users to a site that contains infringing material, such as search engines and online directories.[11]

China has followed the United States legislative model to regulate ISP liability and limitations. Under the 2006 Regulation, there are four categories of ISP conducts under liability limitations subject to certain conditions. Similar to the four categories in Section 512 of the DMCA, the four categories in the Chinese regulation are (1) ISPs which provide automatic access or automatic transmission of copyright works according to the instructions of web subscribers;[12] (2) ISPs which automatically store the works supplied by other ISPs and automatically transmit the works to the subscribers according to the technical arrangement with the purpose to promote network transmission efficiency;[13] (3) ISPs which provide information memory space for subscribers to supply works;[14] and (4) ISPs which provide searching or linking services to service recipients.[15] Although the expressions are different from the corresponding provisions in the DMCA, the four categories of ISP conducts in the 2006 Regulation in fact correspond to the four categories of Section 512 in the DMCA respectively. These statutory classifications of ISP conducts from another aspect indicate

11. *The Digital Millennium Copyright Act of 1998: U.S. Copyright Office Summary*, U.S. COPYRIGHT OFFICE (Dec., 1998), http://www.copyright.gov/legislation/dmca.pdf.

12. Shên Hsi Wang Lao Ch'uan Po Ch'üan Pao Hu T'iao Li [Regulation on the Protection of the Right to Network Dissemination of Information] (promulgated by the St. Council, May 10, 2006, effective July 1, 2006) [hereinafter Regulation on the Protection of the Right to Network Dissemination of Information], art. 20 (China).

13. Regulation on the Protection of the Right to Network Dissemination of Information, art. 21 (China).

14. Regulation on the Protection of the Right to Network Dissemination of Information, art. 22 (China).

15. Regulation on the Protection of the Right to Network Dissemination of Information, art. 23 (China).

that most ISPs at issue are those who merely function as data conduits for facilitating information transmission and dissemination, especially ISPs that want to argue for protection from infringement liability.

### *B. Importance of Establishing Certainty about Liability and Limitations for Internet Service Providers*

The definition and analysis with regard to ISPs show that when ISPs are alleged to commit copyright infringement, the liability that they shoulder is secondary or indirect liability. Since ISPs do not provide copyright contents, they are liable for facilitating the direct copyright infringement of their internet subscribers.

Why is it necessary and important to establish certainty and predictability for the indirect liability of technological intermediaries such as ISPs? There are two reasons. On the one hand, under certain circumstances, it is too costly and difficult for copyright owners to fight against direct infringers, especially when the number of direct infringers is high and direct infringers cannot be easily identified. Indirect liability becomes the only efficient and appropriate means to compensate for the losses of copyright owners. Without indirect liability, copyright owners cannot effectively enforce their exclusive rights in some situations. Therefore, it is necessary to look into the indirect liability of technological intermediaries. On the other hand, digital network technology is a double-edged sword. It can be used for both legal and illegal purposes. It is unfair to hold ISPs liable for the infringement activities of third parties if ISPs are not at fault. That ISPs are strictly held for liability will unreasonably disrupt legitimate activities in information dissemination and impede the development of new technology. Therefore, limitation of indirect liability and safe harbors should be established for ISPs so as to better balance the interests of copyright owners and technological intermediaries, and protect the free flow of information.

## III. INTERNET SERVICE PROVIDER LIABILITY AND SAFE HARBOR RULES ESTABLISHED BY COMMON LAW CASES

### A. *Sony Safe Harbor Rule*

American cases have considerable influence on establishing ISP liability and safe harbors to protect technological intermediaries. Prior to the enactment of the DMCA, the most influential case was *Sony Corporation of America v. Universal City Studios Inc.* which established the famous safe harbor system for technological intermediaries and is still supported by many telecommunication industries and scholars today.

In this case, Universal sued Sony for indirect copyright infringement by claiming that Sony's new invention, the Betamax video cassette recorder (VCR), would result in rampant unauthorized reproduction of their copyrighted motion pictures or TV programs.[16] In 1981, the Ninth Circuit Court of Appeals reached a judgment in favor of Universal, holding that Sony was liable for contributory infringement because of its actual knowledge of the unauthorized copying of TV programs by VCR user for time-shifting purposes and the primary infringement use of VCRs.[17] In the appellate litigation of 1984, the Supreme Court reversed the decision, ruling that Sony was not liable for contributory infringement since time-shifting was fair use and the VCR could be substantially used for non-infringing purposes.[18] The final judgment of the *Sony* case borrowed a staple article of commerce rule from patent law to mitigate the holders of intellectual property and technology developers.

The United States Copyright Act did not expressly render anyone liable for infringement committed by another, when the *Sony* case was carried on.[19] "If secondary liability is to be imposed on Sony, it must rest on the fact that it has sold equipment with constructive knowledge of the fact that its customers may use that equipment to make unauthorized copies of copyrighted material."[20] However, there was "no precedent in the law of copyright for the imposition of vicarious liability on such a theory" at the time.[21] The Supreme Court noticed the analogy of such a problem in patent law. The United States Patent Law expressly regards active inducement of infringement of a patent as contributory infringement. However, contributory infringement is only applicable to "the knowing sale of a component especially made for use in connection with a particular patent".[22] The sale of a staple article or commodity of commerce suitable for substantial non-infringing use will not result in contributory infringement liability,[23] even if the seller actually knows that the article will probably be used for infringement purposes. Uses will be deemed insubstantial in patent law if they are "far-fetched, illusory, impractical, or merely experimental".[24] The courts borrowed the rule in the patent law to explain copyright indirect infringement liability and established the Sony safe harbor that technology developers or sellers should not be contributory liable if the technology will

16. Universal City Studios, Inc. v. Sony Corp. of America, 659 F.2d 963 (9th Cir. 1981).
17. *Sony Corp. of America*, 659 F.2d 963.
18. Sony Corp. of America v. Universal City Studios, Inc., 464 U.S. 417 (1984).
19. *Universal City Studios, Inc.*, 464 U.S. at 434.
20. *Universal City Studios, Inc.*, 464 U.S. at 439.
21. *Universal City Studios, Inc.*, 464 U.S.
22. *Universal City Studios, Inc.*, 464 U.S. at 440.
23. *Universal City Studios, Inc.*, 464 U.S.; 35 U.S.C. § 271(c) (2010).
24. 5 DONALD S. CHISUM, CHISUM ON PATENTS § 17.03[3] (2004).

have substantial non-infringing uses. By drawing up such a conclusive rule, the court aimed to reduce the monopolies of the entertainment industry on articles of commerce that are not subjects of copyright protection.

The Sony safe harbor has been supported by scholars in the face of indirect infringement liability issues brought on by technology development. Even today, many commentators argue that the Sony safe harbor should apply to new digital technologies such as peer-to-peer file sharing technology. As scholars of the Samuelson Law, Technology & Public Policy Clinic at the University of California- Berkeley explained in the Interest of Amici Curiae, "the Sony safe harbor further promotes business certainty and judicial efficiency because of its simplicity, clarity, predictability, and objectivity. It does not require delving into technology developers' states of mind; it does not require extensive evidence or speculation about current and future uses of technologies and in what proportion each use exists or is likely to evolve; and it does not require courts to consider what other kinds of technologies might have been developed instead. Sony simply asks courts to determine whether the technology has or is capable of substantial non-infringing uses".[25]

### B. *Contributory and Vicarious Liability Rules*

In some later cases, technological intermediaries were sued for providing peer-to-peer file sharing technology for internet users to freely upload and download copyright music works without authorization by the copyright owners. The defendants relied on the Sony safe harbor to argue for protection from infringing liability based on the fact that peer-to-peer file sharing technology will have substantial non-infringing uses.

In *A&M Records Inc. v. Napster Inc.*, Napster was sued for facilitating users to make available MP3 music files stored on personal computer hard drives for others to reproduce, search for music files stored in computers of other users and disseminate copies from one computer to another via the internet.[26] Napster defended its immunity from copyright infringement liability based on statutory limitations of ISP liability and the Sony safe harbor. The court rejected Napster's safe harbor defense and ruled against them, because Napster knew or should have known that there would be rampant unauthorized transmission of copyrighted works facilitated by its technology and system.[27] The active inducement of copyright infringement

25. Brief for Deirdre K. Mulligan, as Amici Curiae Supporting Reversal, Stephen J. Barrett M.D., et al. v. Ilena Rosenthal, 51 Cal.Rptr.3d 55 (2006) (No. S122953), *available at* https://www.eff.org/sites/default/files/filenode/Barrett_v_Rosenthal/law_professors_amicus_brief.pdf.

26. A&M Records Inc. v. Napster Inc., 239 F.3d 1004 (9th Cir. 2001).

27. *Napster Inc.*, 239 F.3d.

undermined the possibility of safe harbor protection for Napster despite the fact that the peer-to-peer file sharing technology could be used for legal purposes.

In the *Aimster copyright litigation*, Aimster was also sued by the recording industry for facilitating the swapping of digital copies of music works. More indirectly than Napster, Aimster users swapped music files in an online chat room enabled by an instant messaging service.[28] However, this kind of file sharing did not shelter Aimster from infringing liability, because Aimster actually knew about the infringement activity of its users, and its business model was based on the volume of infringement uses of its technology. In addition, compared with the serious harm to the interests of copyright owners by massive illegal file swapping, the cost of preventing the infringement activity was relatively small.[29]Aimster could not prove that eliminating or substantially reducing the infringing of its customers would be disproportionately costly.[30] Therefore, the court also ruled against Aimster despite its defense based on the safe harbor.

Although subsequent ISPs provided file sharing technology more surreptitiously, they could not avoid being liable for the copyright infringement of their clients either. In *Metro-Goldwyn-Mayer Studio Inc. v. Grokster Ltd.,* Grokster was also sued for indirect copyright infringement due to the unauthorized file-sharing of copyrighted works by their clients. In contrast to the services provided by Napster and Aimster, the software provided by Grokster enabled users to directly swap copyrighted files with each other.[31] There was not a centralized indexing system that facilitated the linking of individual users. Grokster knew about the infringing activity of its customers and financially benefited from the infringing uses. However, when examining Grokster's material contribution and supervision capability, the district court emphasized on their decentralized network system and thus ruled in favor of Grokster. In its ruling, the court also mentioned the potential non-infringing uses of Grokster technology, such as distribution of copyrighted works under authorization or of public domain works.[32] In the appellate litigation, the Ninth Circuit confirmed the decision of the district court, believing that the lack of control over the direct infringement of the users and the existence of potential non-infringing uses were sufficient enough to protect Grokster from secondary liability. Nevertheless, in the final judgment reached by the Supreme Court, the decisions of the lower courts were overturned. The Supreme Court ruled against Grokster,

28. *In re* Aimster Copyright Litigation 334 F.3d 643 (7th Cir. 2003).
29. *Aimster Copyright Litigation*, 334 F.3d 643.
30. *Aimster Copyright Litigation*, 334 F.3d 643.
31. Metro-Goldwyn-Mayer Studios Inc. v. Grokster Ltd., 380 F.3d 1154 (9th Cir. 2004).
32. *Grokster Ltd.*, 380 F.3d.

explaining that Grokster's intent of active inducement of copyright infringement could not shelter them under the safe harbor and the fact that the so-called potential non-infringing uses only accounted for ten percent of all uses also refuted Grokster's defense under the safe harbor.[33]

In all of the above-mentioned cases, the courts denied the claim by ISPs to use the Sony safe harbor and relevant statutory limitations on liability and ruled in favor of the recording industries. The most important reason is that ISPs in these cases could supervise or control the consumption of their services by internet users and actively discourage the infringing activity. In contrast, Sony was not able to supervise or control the use of their products after the Betamax VCRs were sold, although Sony could expect that such products would be used for infringing purposes. Therefore, ISPs that provide peer-to-peer file sharing technology should be rendered liable for direct copyright infringement by their internet users despite the potential non-infringing uses of the technology. Vicarious and contributory liabilities which are applicable to ISPs have been developed from these judicial decisions.

To be held liable under the contributory liability rule, three terms need to be satisfied: (1) there should be direct infringement by a primary infringer; (2) the ISP should know or have awareness of the direct infringement; and (3) the ISP should have made a material contribution to the infringement. To be held liable for vicarious infringement, there are also three terms that need to be met: (1) there should be direct infringement by a primary infringer; (2) the ISP obtained direct financial benefits from the primary infringer; and (3) the ISP has the right and ability to supervise or control the activity of the primary infringer. In the three terms, the ISPs were held either contributory or vicariously liable for the infringement of their internet users because they all knew about the illegal reproduction and distribution of copyright works by their subscribers, actively endorsed and contributed to the infringement, and had the ability to cease the infringement activities. Some ISPs such as Aimster, even obtained financial benefits from the infringing uses.

Although vicarious and contributory liability have developed from judicial decisions, certain factors including the knowledge of ISPs of direct infringement, obtaining direct financial benefits from the direct infringer and having the ability to supervise or control direct infringement have been incorporated into both American and Chinese digital copyright statutes and regulations. For example, under the third and fourth categories of ISP conducts in Section 512 of the DMCA, namely, the "storage of information on systems or networks at direction of users" and "information location

33. Metro-Goldwyn-Mayer Studios Inc. v. Grokster Ltd., 545 U.S. 913 (2005).

tools", ISPs must satisfy certain conditions in order to be safeguarded from infringing liability. These conditions are as follows: (1) the ISP does not have actual knowledge that the material or activity is infringing or in the absence of such actual knowledge, is not aware of the fact that there is apparent infringing activity;[34] (2) the ISP does not receive any financial benefits that are directly attributable to the infringing activity, if the ISP has the right and ability to control such activity;[35] and (3) upon receiving notification with regard to infringing activity, the ISP expeditiously removes or disables access to the alleged infringing material.[36] Similarly, in relation to the third category of ISP conducts, the supplying of information memory space to subscribers, the 2006 Regulation of China had also established almost the same conditions for protection from liability: (1) the ISP does not know or have justifiable reasons to know about the infringing activities of the subscribers; (2) the ISP does not obtain any economic benefits from the infringing activity; and (3) the ISP removes the works in question upon receiving notice from the copyright owners.[37] Besides the requirement to expeditiously remove the alleged infringing material, other factors are a combination of vicarious and contributory liability established in American law cases. Detailed situations with regard to these factors need to be examined so as to establish certainty and predictability of ISP liability and safe harbors.

1. *Knowledge or Awareness of Direct Infringement*

Although ISPs do not have the obligation to actively monitor subscribers in the use of their services, they should not have actual knowledge or awareness of the circumstances in which infringing activity is apparent. Once they have this knowledge or awareness, the ISPs should expeditiously remove or disable access to the material. Ignorance about the infringement will definitely not safeguard the liability of ISPs. ISPs should not have an awareness of the apparent infringement either. What constitutes apparent infringement thus becomes the determinative factor on whether the liability of ISPs can be safeguarded.

Professor Jane Ginsburg concluded in her article the possible situations under which infringement is deemed apparent in a few cases. These possible situations that "warrant service provider's vigilance might include abnormally and disproportionately high traffic to the area of the site where

34. 17 U.S.C. §§ 512(c)(1)(A) & 512(d)(1).
35. 17 U.S.C. §§ 512(c)(1)(B) & 512(d)(2).
36. 17 U.S.C. §§ 512(c)(1)(C) & 512(d)(3).
37. Regulation on the Protection of the Right to Network Dissemination of Information, art. 22 (China).

the alleged infringement is located, or the appearance of terms like 'pirated' or 'bootleg' in the name of the file".[38] In addition, if "the file title includes the name of a motion picture, television program, or sound recording of which the person or entity posting the content is obviously not the copyright owner" and the title is the subject of "repeated section 512(c) 'take down' notices" sent by copyright owners, such files are blatant enough for ISPs to note and take action.[39] These situations can also be deemed as justifiable reasons for ISPs to be aware of the infringement under the Chinese regulation.

Further explanations regarding constructive knowledge in China was included in the Provisions on Certain Issues Related to the Application of Law in the Trial of Civil Cases Involving Disputes over Infringement of the Right to Network Dissemination of Information (thereafter, the Provisions) which was released by the Supreme Court in November 2012 and took effect from January 1st, 2013. Article 9 of the Provisions lists 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 works, performance and audio-visual recordings disseminated and the degree of the obviousness of the infringement; (3) whether the ISP actively selects, edit, modify or recommend the works, performance and audio-visual products; (4) whether the ISP has taken positive and reasonable measures to prevent infringement; (5) whether the ISP has set up a 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. Such list of factors aims to interpret constructive knowledge from multi-perspectives, including notice and takedown procedure as well as adoption of technological measures by ISPs. It would be better implementable if detailed situations discussed above are used as examples to provide supplementary explanation of the obviousness of infringement.

However, in order not to impose excessive responsibility onto the ISPs, the American court decisions also expressively emphasized that "general knowledge that infringement is ubiquitous does not impose a duty on the service provider to monitor or search its services for infringement".[40] Mere knowledge of the prevalence of infringing activity in general is not enough to prove that the ISPs have actual knowledge or awareness of the

38. Ginsburg, *supra* note 8, at 191.
39. Ginsburg, *supra* note 8, at 192.
40. Viacom Intern, Inc. v. YouTube, Inc., 718 F. Supp. 2d 514 (2010).

infringement.[41] Knowledge and awareness should be specific to particular individual circumstances.[42] In addition, if the material offered by subscribers on its surface does not clearly reveal signs of infringement, such activity is not sufficiently apparent as infringing and service providers do not need to conduct further investigations.[43]

2. *Direct Financial Benefits from Direct Infringement*

As to whether ISPs obtain direct financial benefits or any economic benefits from the primary infringement, the determinative factor is based on the relationship between the infringement and benefit.

When the benefits that the ISPs gain are immensely associated with the infringing activity of the subscribers, it will not be difficult to determine that these are direct benefits. For example, if advertising accepted by a website targets infringing material, then the benefit is very obvious.[44] However, when the benefit is not so closely related to the infringing activity, it will be more difficult to determine whether the benefit is direct or not. Also, by using website advertising as an example again, if the rates charged do not target the infringing material, but to the popularity of the material as a whole with the advertising, it cannot be simply assessed that there is a direct benefit by assuming that the infringing material enhances the overall popularity of the website.[45] Furthermore, the need to conduct an investigation on whether the website popularity is caused by infringing material will increase ISP liability, because further investigation will clearly inform ISPs or provide them with the awareness of infringement which previously, was not so obvious. Actual knowledge or awareness will eliminate the safe harbor provision that these ISPs would have originally enjoyed.

Therefore, in order to safeguard proper safe harbor protection for ISPs, benefits to service providers need to be directly associated with the infringing material. Any ambiguity between financial benefit and infringing activity will mean that there are no "direct financial benefits". If copyright owners wish to request the assistance of ISPs to cease infringement, they will need to follow statutory procedures in forwarding copyright infringement notifications to the ISPs to start the process of information removal.

41. *YouTube, Inc.*, 718 F. Supp. 2d.
42. *YouTube, Inc.*, 718 F. Supp. 2d.
43. Ginsburg, *supra* note 8, at 192-93.
44. Ginsburg, *supra* note 8, at 194.
45. Ginsburg, *supra* note 8, at 194-95.

3. *Right and Ability to Supervise or Control Infringing Activity*

Even if an ISP had obtained direct financial benefits from the primary infringement, they cannot be denied safe harbor protection if they do not have right and ability to control the infringing activity. The circumstances that influence whether ISPs have control over infringement can be interpreted in various ways. The first interpretation is that ISPs have "the right and ability to control" if they can block the use of their services for infringing purposes.[46] This interpretation is supported by the common law rule of vicarious liability. The second interpretation is that the mere blocking of access to the infringing material does not indicate that the ISPs have the ability to control[47] because "[the] ability to intervene before the infringing content is placed on the website" is also required under Section 512 of the DMCA.[48]

In the first interpretation, the requirement for ISPs to have "the right and ability to control" will automatically disqualify them for safe harbor protection because under the notice and takedown regime, almost all ISPs are able to subsequently block access to alleged infringing material upon receiving notifications from the copyright owners. The simple interpretation of "the right and ability to control" as taking subsequent measures to cease infringement will result in most ISPs being held liable for the infringing activities of their subscribers. The second interpretation, however, is more appropriate to define the ability to control, since the ability to intervene before the infringing material is posted online also implies that the ISP has knowledge or awareness of the infringement. Therefore, it is better to interpret "the right and ability to control" as a prerequisite to intervene with the infringement of subscribers so as to comply with the combined immunities of indirect liability and safe harbors.

C. *Authorization or Joint Tortfeasor Liability of Commonwealth Jurisdictions*

Similar to vicarious and contributory liability, some of the Commonwealth jurisdictions, such as Australia, the United Kingdom and Hong Kong, have also developed indirect liability doctrines, such as those that deal with authorization or joint tortfeasor liability for technological intermediaries through various cases and statutory supplements.

46. Ginsburg, *supra* note 8, at 193-94.
47. Ginsburg, *supra* note 8, at 196.
48. *Id.*

1. *Liability by Authorization*

In these Commonwealth jurisdictions, the infringement of the exclusive rights of copyright owners can be realized in two ways, direct and indirect. Technological intermediaries will be regarded as directly liable if they have a role in determining the content of the communication where copyright infringement is found. Even if the technological intermediaries do not play a part in determining the contents of the communication, they are indirectly liable if they have authorized infringing activity by third parties. "Authorization" for cases in both Australia and the United Kingdom is defined by the courts with an ordinary dictionary definition of "sanction[ing], approv[ing] and countenance[ing]"[49] After they analyzed various cases, Professors Jane Ginsburg and Sam Ricketson concluded that "authorization" in the Commonwealth judicial sense not only includes specific granting of permission, but should also contain implications from surrounding circumstances that allow a suspect to carry out an infringing act.[50] The inference may be determined case by case. In order to draw the correct implication from the actions of the defendants, relevant facts in each case should be very carefully examined.[51]

Since liability by authorization may increase the possibility of holding the intermediaries indirectly liable, Australian courts have developed a series of common law rules to limit broad explanations with regard to issues around authorization or permission. First, in order to be liable for the copyright infringement of a third party, the alleged authorizer must have some ability to control the use of its services. In *University of New South Wales v. Moorhouse*, the defendant or the university was not held liable for providing photocopy machines in its library for making copies, which was deemed to be infringing, because the university did not set up control mechanisms on who could use the copiers.[52] In later cases,[53] defendants were sued for manufacturing and offering tape-recording facilities for consumers to make infringement copies of sound recordings. However, none of these defendants were charged for liability by authorization, because they did not have any control over the use of their products after the sale. Thus,

49. Falcon v. Famous Players Film Co. Ltd. [1926] 2 K.B. 474 [hereinafter *Falcon*]; University of New South Wales v. Moorhouse 133 CLR 1 (1975) [hereinafter *University of New South Wales*].

50. Jane Ginsburg & Sam Ricketson, *Inducers and Authorisers: A Comparison of the US Supreme Court's Grokster Decision and the Australian Federal Court's KaZaa Ruling*, 11 MEDIA & ARTS L. REV. 1, 11 (2006).

51. *Id*.

52. *Falcon* and *University of New South Wales*, *supra* note 49.

53. *WEA International Inc. v Hanimex Corporation Ltd*. (1987) 10 IPR 349 (Austl.); RCA Corp v. John Fairfax & Sons Ltd, [1982] R.P.C. 91; *Australian Tape Manufacturers Ltd. v Commonwealth of Australia* (1993) 25 IPR 1(Austl.).

the provision of potential opportunities to commit infringement or encouraging the act of infringement is insufficient. There needs to be some actual association between the intermediaries and direct infringers. Secondly, the alleged authorizer must have some degree of knowledge of the infringement. The courts have refused to determine liability by authorization if no action was carried out because the defendant did not know or had any reason to suspect that an infringement act may have been carried out.[54] Otherwise, it would be concluded that the defendant had authorized the infringing activity, if s/he knew or had reason to suspect that infringing activity was being carried out or likely to be carried out.[55] The third rule may be inferred from the second rule with regard to the knowledge of the intermediaries about the infringement: if a defendant anticipates that infringing activity may take place due to the facilitation of his/her services and takes reasonable measures to avoid this from happening, s/he will thus not be held liable.

These rules developed by various cases were amended and incorporated into the Australia Copyright (Digital Agenda) Amendment Act in 2000 which revised the Australian copyright regime to adapt to the digital network environment. Under Section 36(1A) of this copyright act, several factors are listed which must be taken into consideration when judging whether a defendant has authorized any act that infringes copyright: (1) the extent (if any) of the person's power to prevent the infringement; (2) the nature of any relationship that exists between the person and the direct infringer; and (3) whether the person took any reasonable steps to prevent or avoid the infringement, including whether the person complied with any relevant industry codes of practice.[56] By codifying the rules developed in the various cases, the Copyright Amendment Act 2000 aims to establish legislative certainty on liability for authorizing infringements.[57]

Despite the different expressions, the Australian cases and statutory factors make liability by authorization more closely resemble vicarious and contributory liability under the United States legal system. The first and third provisions of the statute focus on the ability of the intermediaries to control infringing activity and subsequent takedown action after finding out about the infringement. The second provision, the relationship between the intermediary and the direct infringer, implies many situations that need to be taken into consideration, such as whether the intermediary knows or is aware of the direct infringement, or whether the intermediary gains financial benefits from the suspected infringing activity. For example, in cases that

54. *Australasian Performing Right Association Ltd. v Jain* (1990)18 IPR 663 (Austl.).
55. *University of New South Wales*, *supra* note 49.
56. *Australia Copyright (Digital Agenda) Amendment Act 2000* (Cth) s 36(1A) (Austl.).
57. Explanatory Memorandum, Copyright Amendment (Digital Agenda) Bill 1999 (Cth) (Austl.).

involve tape-recording, the relationship between the apparatus vendor and buyer comes to an end when the apparatus has been sold. However, under the digital network environment, the relationship between the providers of peer-to-peer file sharing technology and subscribers continues, as long as the service providers maintain the administration of the websites and offer upgrades or technical assistance. The service providers may also continue a relationship with the subscribers if they are financially benefited from advertising which targets to the hits on the online material.

### 2. *Joint Tortfeasor Liability*

Joint tortfeasor liability is similar to contributory liability under the United States common law, as it punishes the assisting, abetting, facilitating and inducement of the commission of infringing acts.[58] However, joint tortfeasor liability is different in that there is an additional requirement for the participation of the intermediary with the direct infringer in furthering a common design to commit infringement, which narrows the scope of acts that can be deemed as indirect infringement because it is difficult to prove common design.

Under the principle of joint tortfeasor liability, the ISPs that provide peer-to-peer file sharing technology will not be held liable for the infringement of their subscribers. The ISPs merely supply the technology and services for facilitating data transmission and information dissemination. Such technology can be used for both legitimate and illegitimate purposes. It will be quite difficult to determine the presence of a common design between ISPs and their subscribers with the aim to upload and download copyright files. However, liability by authorization is a different matter. Even though ISPs are not joint tortfeasor liable due to the absence of a common design with their subscribers, ISPs may be liable by authorization if they have reason to know and own the ability to prevent the infringement, but did not take any reasonable measures to stop the infringement. In other words, although joint tortfeasor liability limits the possibility of holding ISPs indirectly liable, liability by authorization restores this possibility by codifying conditions developed from various cases.

## IV. INTERNET SERVICE PROVIDER LIABILITY AND SAFE HARBOR RULES ESTABLISHED BY STATUTES

Besides the principles of indirect infringing liability and safe harbor rules developed from common law cases, legislatures among different

58. Ginsburg & Ricketson, *supra* note 50, at 15.

jurisdictions have also created statutory conditions that limit the liability of ISPs. In order to be protected from vicarious or contributory liability or liability by authorization, ISPs must follow the statutory notice and takedown regime which was first legitimized in the United States legal system.

### A. *Notice and Takedown Regime*

Upon receiving proper notification from copyright owners under the notice and takedown regime, ISPs must promptly remove or block access to alleged infringing material identified in the notification. Once the takedown requirements have been immediately satisfied, an ISP is exempted from liability.

Section 512 in the DMCA of the United States has established detailed procedures on how ISPs receive notifications, the elements of a qualified notification and the actions taken by ISPs after receiving proper notification. First, an ISP must designate an agent to receive notifications of infringement claims. The ISP shall make available to the public both on its website and by providing to the Copyright Office the name, address and contact information of the designated agent.[59] Secondly, the infringed party must file a qualified notification including a list of specified items to the agent that informs the ISP about the infringement. The list of items that contribute to an effective notification include: (i) the signature of the person authorized to act on behalf of the owner whose exclusive right has been allegedly infringed; (ii) identification of the copyrighted works that have been infringed or a representative list of such works if multiple works are on a single website; (iii) identification of the materials that have been infringed and information to permit the ISP to locate the said materials; (iv) provision of the accuser's contact information; (v) a statement that clarifies the good faith of the accuser; and (vi) a statement that verifies the accuracy of the information under the penalty of perjury.[60] A notification that fails to include these items will not be considered when determining the actual or constructive knowledge of the ISP, and thus may waive the responsibility of the ISP to perform a takedown.[61] Finally, the ISP should act expeditiously to remove or disable access to the material once they receive proper notification. Regardless of the notice and takedown regime, Section 512 does not require ISPs to affirmatively monitor their services or actively disable access to the suspected infringing material in order to qualify for the statutory safe harbor

59. 17 U.S.C. § 512(c)(2).
60. 17 U.S.C. § 512(c)(3)(A).
61. 17 U.S.C. § 512(c)(3)(B).

protection.[62]

By assimilating Section 512 of the DMCA, China also incorporated the notice and takedown regime in its 2006 Regulation through legal transplant. If copyright owners believe that works which are accessed through the ISP services are an infringement of their right to network dissemination of information, they can file a notice to the ISP and require them to delete or block access to the works concerned.[63] The notice should contain the name and contact information of the copyright owner; names and hyperlinks of the works concerned; and preliminary evidence of infringement.[64] Once the notice has been received from the copyright owner, the ISP should immediately delete or block access to the works that are suspected of infringement and notify the subscriber involved in the infringement.[65] If the notification cannot be sent to the subscriber, the content of the notification should be published on the information network.[66]

Although other jurisdictions have not incorporated the notice and takedown regime as opposed to the United States and China, they all include relevant provisions in their statutes that prompt ISPs to expeditiously remove or disable access to the concerning materials if the ISPs actually know or are aware of the illegal activity. Such provisions appear in the European Union Directive on Electronic Commerce, the Electronic Commerce Regulations 2002 of the United Kingdom, and the Copyright (Digital Agenda) Amendment Act 2000 of Australia. Australia later incorporated the notice and takedown regime after signing the Australia-United States Free Trade Agreement in 2004. The obligation of implementing the agreement led to the enactment of the Copyright Amendment Act 2006 under which ISPs are to act in accordance with the notice and takedown regime, and comply with the requests of copyright owners to prevent infringement so as to safeguard themselves from liability.

The notice and takedown regime in the United States, China and Australia and the immediate takedown provision in other jurisdictions facilitate copyright owners to effectively supervise online material and remove suspected infringing copies via cooperation with ISPs. This sort of legal system will efficiently address copyright infringement in the digital network environment at a low cost. This is especially true if the notice and takedown regime has established detailed procedures and conditions which copyright owners and ISPs can easily follow. However, immediate takedown

62. 17 U.S.C. § 512(m).

63. Regulation on the Protection of the Right to Network Dissemination of Information, art. 14 (China).

64. *Id.*

65. Regulation on the Protection of the Right to Network Dissemination of Information, art. 15 (China).

66. *Id.*

requirements in the system will increase the risk of errors, which may result in the removal or blocked access of legitimate works. Thus, Section 512 of the DMCA has also established a "counter notification" regime which may help to remedy the losses suffered by ISPs and their subscribers due to erroneous takedowns.

### B. *Counter Notification Regime*

The counter notification regime allows subscribers to request ISPs to recover links to their works if proven that the works in question have not committed infringement. Similar to the notice and takedown regime, several steps should also be followed. First, the ISP shall notify the subscriber that the material has been taken down.[67] Secondly, the subscriber needs to submit a proper counter notification in order for the removed material to be reinstated. Similar to the items found in a proper notification, a counter notification also needs to satisfy several conditions, including providing the signature of the subscriber, identifying the removed material, providing a statement of the good faith of the subscriber under the penalty of perjury, and submitting the name and contact information of the subscriber.[68] Thirdly, upon receiving the counter notification, the ISP shall inform the subscriber that they will reinstate the removed material in 10 business days.[69] Finally, the ISP shall reinstate the material which has been removed or blocked in no less than 10 days, no more than 14 business days, after receiving the counter notice.[70]

The counter notification regime has also been transplanted into China but with subtle variations. The counter notification in China must include the following: name and contact information of the subscriber; name and hyperlink addresses of the works that are requested for recovery; and the preliminary evidence on non-infringement.[71] After receiving the counter notification, the ISP should immediately reinstate the deleted works or the hyperlink to the works and deliver the counter notification to the copyright owner.[72] After receiving the counter notification, the copyright owner cannot request the ISP to delete or block access to the works concerned again.[73] Furthermore, the copyright owner will be charged for compensation

67. 17 U.S.C. § 512(g)(2)(A).
68. 17 U.S.C. § 512(g)(3).
69. 17 U.S.C. § 512(g)(2)(B).
70. 17 U.S.C. § 512(g)(2)(C).
71. Regulation on the Protection of the Right to Network Dissemination of Information, art. 16 (China).
72. Regulation on the Protection of the Right to Network Dissemination of Information, art. 17 (China).
73. *Id.*

liability if the erroneous takedown resulted in any losses to the subscriber.[74]

The establishment of a counter notification regime balances the interests of ISPs and subscribers to a certain degree against copyright owners by providing the opportunity for suspected infringers to dispute the issue and remedy any erroneous takedowns. China even grants monetary compensation to innocent subscribers. This type of legal system is a great leap in achieving a balance of interest between copyright owners and internet consumers. However, counter notification alone cannot entirely eliminate the negative effects brought upon by an immediate takedown, because the provisions do not give any detailed explanations with regard to the exact period of time which would constitute as "immediate". Under an immediate takedown requirement, the suspected subscriber may not have the chance to defend him/herself before his/her material is removed or has access blocked. In addition, it will be costly for individual users to collect evidence to prove their innocence when facing censure from powerful entrepreneurial copyright holders. The immediate takedown requirement will also place ISPs in a dilemma: if they cooperate with copyright owners to expeditiously take down the alleged infringing material, they will face the risk of losing customers; if they delay the removal of suspected infringing material to protect current or potential customers, the ISPs will lose the statutory safe harbor protection.

### C. *Subpoena Procedure or Norwich Pharmacal Order*

In addition to the notice and take-down regime and counter notification, the DMCA also includes a subpoena procedure under which the copyright owner may request a district court to issue a subpoena to an ISP to identify an alleged infringer.[75]

In order to initiate a subpoena under the DMCA, copyright owners should first file a request to the district court clerk which contains a notification, including the same items that are in the notice and takedown regime, the proposed subpoena and a sworn declaration that the information released by the clerk will only be used for copyright protection.[76] After receiving the abovementioned documents, the district court clerk will expeditiously issue and sign the subpoena, and deliver the document to the ISP for disclosure of the requested information.[77] Upon receiving the subpoena, the ISP should immediately disclose the concerned information to

74. Regulation on the Protection of the Right to Network Dissemination of Information, art. 24 (China).

75. 17 U.S.C. § 512(h)(1).

76. 17 U.S.C. § 512(h)(2).

77. 17 U.S.C. §§ 512(h)(3)-(4).

the copyright owner.[78]

The subpoena procedure could help copyright owners collect pivotal information with regard to suspected infringers with the purpose of establishing reliable evidence, thus better addressing online copyright infringement. Nonetheless, there is negative impact in the subpoena procedure on the protection of the personal privacy of internet users. The procedure may be abused by copyright owners to collect whatever information they want on internet subscribers, even information that is not relevant to copyright protection.

China has not imported the American subpoena procedure. Instead, the administrative departments of copyright are empowered to demand an ISP to disclose information, such as the name, contact information and web address of the subscriber who is suspected of infringement.[79] If the ISP does not cooperate or delays disclosing relevant information without a justifiable reason, the administrative departments can give a warning to the ISP or more seriously, confiscate the equipment that is used to facilitate the supply of infringing material.[80] In comparison to the subpoena procedure in the United States, there is less protection of the privacy of subscribers in China due to administrative power abuse.

Commonwealth jurisdictions, such as the United Kingdom and Hong Kong, have incorporated the Norwich Pharmacal judicial order in their legal system. In these jurisdictions, courts can order individuals who have information that may lead to the identification of the defendant to disclose that information.[81] In the Preliminary Proposals for Strengthening Copyright Protection in the Digital Environment released by the Hong Kong government in 2007 after launching a public consultation, Hong Kong aims to maintain the current Norwich Pharmacal discovery procedure in its copyright protection system. Under the Norwich Pharmacal procedure, copyright owners can obtain a court order that requires ISPs to disclose the source of the alleged infringing material.[82] In contrast to the subpoena procedure which allows copyright owners to request a subpoena at any time, the court will not exercise the Norwich Pharmacal procedure unless the individual who is seeking a court order has a genuine intent to commence a

78. 17 U.S.C. § 512(h)(5).

79. Regulation on the Protection of the Right to Network Dissemination of Information, art. 13 (China).

80. Regulation on the Protection of the Right to Network Dissemination of Information, art. 25 (China).

81. *Norwich Pharmacal Orders: A Quick Guide*, PRACTICAL LAW, http://ld.practicallaw.com/0-211-3137 (last visited Sept. 1, 2011).

82. *Preliminary Proposals for Strengthening Copyright Protection in the Digital Environment*, H. K. COMM. & ECON. DEV. BUREAU (Apr., 2008), http://www.ipd.gov.hk/eng/intellectual_property/copyright/Consultation_Document_Prelim_Proposals_Eng(full).pdf.

proceeding and the proceeding cannot be commenced without information on the defendant.[83] Therefore, personal online privacy will be more safeguarded. Even though some have commented that the Norwich Pharmacal procedure is too slow and costly, the Hong Kong government is opposed to adopting more convenient procedures in case the personal privacy of internet users cannot be guaranteed.

The Norwich Pharmacal discovery procedure is widely used by copyright owners to identify direct infringers in the digital network environment. In *Dish Network LLC & Others v. Zentek International Co. Ltd. & Another* judged by the Hong Kong High Court, the plaintiffs who were North American satellite broadcasters, applied for the Norwich Pharmacal order against the defendant, a Hong Kong company and its director who hosted services for websites that provided pirated computer software for subscribers to use in descrambling the encrypted programs of the plaintiffs.[84] The plaintiffs sought for the Norwich Pharmacal order to compel the defendants to disclose the identity and information of the owners and subscribers of the websites so as to advance the proceeding against the primary infringers. The court finally approved the Norwich Pharmacal procedure, and ordered the defendant to disclose the requested information.

## V. NEW CONDITIONS FOR SAFE HARBORS ON INTERNET SERVICE PROVIDER LIABILITY: GRADUATED RESPONSE

Despite that there is the notice and takedown regime and subpoena or the Norwich Pharmacal discovery procedures, copyright industries continue to lobby governments to adopt more aggressive and strict anti-counterfeiting policies to address copyright infringement in the digital network environment. A new policy with regards to ISP liability that has been recently adopted by some jurisdictions is "three strikes and you're out" or the "graduated response" policy which allows ISPs to disconnect the internet access of the alleged infringer after sending several warnings to the infringer about the suspected infringing activity.

The graduated response system was originally known as "three strikes and you're out" which originated from baseball.[85] However, the term "three strikes" could easily be misunderstood to be associated with physical assault and violence. In addition, this is erroneous with regard to the number of

83. *Supra* note 81.

84. Dish Network LLC v. Zentek International Co. Ltd. [2009] 3 H.K.C. 52 (C.F.I.), *available at* http://www.hklii.hk/cgi-bin/sinodisp/eng/hk/cases/hkcfi/2008/887.html?stem=&synonyms=&query=title(Dish%20Network%20LLC.

85. *Graduate Response*, WIKIPEDIA, http://en.wikipedia.org/wiki/Graduated_response (last visited Sept. 1, 2011).

strikes, because the number of warnings will vary according to the legal systems in different jurisdictions. The phrase is inappropriate because of the consequence. In baseball, when a player has been struck out, he may get another chance to go to bat and can also keep playing in the field.[86] In contrast, a repeat infringer may not have another chance to go to bat. The suspected infringer may not have the opportunity to keep playing in the field. Therefore, "graduated response" is a more appropriate term to reflect the continuous and stepwise actions of ISPs against suspected infringers.

### A. *Graduated Response Approach*

Under the graduated response system, an ISP can take a wide variety of actions in warning internet users about their potential copyright infringing activity. These actions may vary among different jurisdictions, including "suspension or termination of service, capping of bandwidth, and blocking of sites, portals and protocols".[87] Among these actions, suspension or termination of internet services is the most severe sanction against the potential infringement.

The European Data Protection Supervisor summarized the graduated response approach in detail.

> "Under three strikes Internet disconnection policies copyright holders using automated technical means, possibly provided by third parties, would identify alleged copyright infringement by engaging in monitoring of Internet users' activities, for example, via the surveillance of forums, blogs or by posting as file sharers in peer-to-peer networks to identify file sharers who allegedly exchange copyright material. 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."[88]

---

86. Michael Weinberg, *Three Strikes, Exile, and Judge Dredd*, PUBLIC KNOWLEDGE (Feb. 1, 2010), http://www.publicknowledge.org/node/2877.

87. Peter K. Yu, *The Graduated Response*, 62 FLA. L. REV. 1373, 1374 (2010).

88. *Opinion of the European Data Protection Supervisor on the current negotiations by the European Union of an Anti-Counterfeiting Trade Agreement (ACTA)*, 2010 O.J. (C147)1 ¶¶ 21 & 22, *available at* http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions

The graduated response system was adopted by various jurisdictions, including France, the United Kingdom, New Zealand, South Korea and Taiwan as legislations and by Ireland as a private ordering. Australia and Singapore assimilated the graduated response system and released their policies that copyright infringers can be disconnected from the internet under judicial procedure.[89] Despite the widespread adoption or support, this policy was met with opposition by many jurisdictions, such as Germany, Spain, Sweden and Hong Kong.

Among the supporting jurisdictions, France is representative of the policy. In May 2009, the French government passed a new law named *Law Promoting the Distribution and Protection of Creative Works on the Internet (Creation and Internet Act)* to implement the graduated response policy.[90] The law was initially rejected by the Constitutional Council due to its violation of a constitutional basic right, the right of communication and expression, but was later revised and thus approved by the Constitutional Council. The law became effective on January 1, 2010.[91] The Creation and Internet Act established an administrative authority, the High Authority for the Dissemination of Works and the Protection of Rights on the Internet (HADOPI), to monitor online copyright infringement and the implementation of the graduated response policy.[92] Upon receiving a complaint from the copyright owner, including the IP addresses and infringing activity of the suspected infringing users, the HADOPI will notify the relevant ISPs and the latter will warn the alleged infringers. The first warning is sent by email which requires the subscribers to cease the infringement. Upon receiving a second complaint from the copyright owners which includes the same IP addresses within six months after the first complaint, the HADOPI will once again notify the ISPs and the latter will send a second warning by regular mail. When a third complaint is received by the HADOPI which involve the same IP addresses within one year after the second complaint, the ISPs will send a third warning which will result in the implementation of a special judicial procedure held by a single judge against the subscribers. The judgment may enforce a fine against the subscribers or the suspension of the access of the subscribers to the internet for two months and up to one year.

---

/2010/10-02-22_ACTA_EN.pdf.

89. Eldar Haber, *The French Revolution 2.0: Copyright and the Three Strikes Policy*, 2 J. SPORTS & ENT. L. 297 (2010).

90. *Id.*

91. *Id.*

92. Stephen W. Workman, *Internet Law-Developments in ISP Liability in Europe*, INTERNET BUSINESS LAW SERVICES (Aug. 24, 2008), http://www.ibls.com/internet_law_news_portal_view.aspx?id=2126&s=latestnews (last visited Sept. 1, 2011).

Although some European countries have actively adopted the graduated response system into their national laws, the European Union was reluctant to incorporate this system into the Anti-Counterfeiting Trade Agreement (ACTA), a new plurilateral treaty that improves global standards for the enforcement of intellectual property rights.[93] According to a European Commission spokesperson who was interviewed before the finalization of the ACTA, the ACTA would not demand that countries disconnect individuals from the internet due to illegal downloads.[94] "The 'three-strike rule' or graduated response systems are not compulsory in Europe".[95] The European Commission wanted to maintain flexibility so that different countries could adopt different approaches.[96] In the finalized version of the ACTA released in November 2010, there is no graduated response policy. In addition, in Section 5 on the enforcement of intellectual property rights in the digital environment, the provisions indicate that the enforcement procedures shall be implemented in a manner that avoids the creation of barriers to legitimate activity and preserves fundamental principles such as freedom of expression, fair process, and privacy.[97] Similarly, the Hong Kong government expressed in its copyright reform proposal for the digital environment that it is not an opportune time to consider the introduction of a graduated response system in Hong Kong, "especially when its implications are yet to be fully tested in overseas jurisdictions".[98]

The adoption of a graduated response system will have both positive and negative impacts on copyright owners, ISPs and internet users. Before importing the system into national legislations, a jurisdiction should carefully analyze whether the positive outweighs the negative or vice versa.

### B. *Impacts on Copyright Owners*

The graduated response system was created through the endeavor of copyright industries to address rampant online copyright infringement, and thus, will greatly benefit copyright owners. First, the graduated response system can prevent repeated copyright infringement and cultivate public respect for intellectual property rights. As the internet has already become a

93. Anti-counterfeiting Trade Agreement (2011), *available at* http://trade.ec.europa.eu/doclib/docs/2011/may/tradoc_147937.pdf.

94. David Meyer, *Europe 'Will Not Accept' Three Strikes in ACTA Treaty*, ZDNet (Feb. 26, 2010), http://www.zdnet.co.uk/news/networking/2010/02/26/europe-will-not-accept-three-strikes-in-acta-treaty-40057434/.

95. *Id.*

96. *Id.*

97. *Supra* note 93, art. 5, ¶¶ 2-4.

98. *Proposals for Strengthening Copyright Protection in the Digital Environment*, H. K. COM. & ECON. DEV. BUREAU (Apr., 2008), http://www.legco.gov.hk/yr09-10/english/panels/ci/papers/ci1117cb1-341-8-e.pdf.

part of people's lives in their work, acquiring of information, entertainment, communication and establishing of friendships, many internet surfers, especially young people, are concerned about being disconnected from the internet. Upon receiving the first or second warning from the ISP, a large number of internet users may stop their infringing activity, in fear that they will be isolated from society. A test in the United Kingdom showed that 70 percent of internet users stopped infringing after the first warning and a further 16 percent stopped after the second warning.[99] This effective type of deterrence will reestablish respect for intellectual property law. Secondly, the graduated response system is an effective and inexpensive means to address and control rampant online copyright infringement. It can reduce a large amount of spending that has been used on massive lawsuits. Compared with imposing indirect liability on ISPs or direct liability on internet users, the graduated response system can be economically efficient as there is a reduction in the launching of costly and time-consuming lawsuits. At the same time, the policy suffocates infringing activity by cutting off the channel that is used to facilitate infringement.

The impacts of the graduated response system on copyright owners seem to be all positive because peer-to-peer file sharing technology facilitates the unauthorized dissemination of copyright works, thus negatively affecting the interest of copyright owners. This assumption misses the fact that file-sharing technology may benefit some authors and artists, especially starters who mainly want to establish their reputation rather than earn money. File-sharing technology can distribute works of artists quickly and cheaply thus increasing their exposure.[100] Broader exposure will in turn increase concert ticket sales and other merchandise.[101] The deterrence brought on by the graduated response system will decrease the use of file-sharing technology and negatively affect certain authors and artists.

Although there may be some negative effects from the graduated response policy on copyright owners, the positive outweighs the negative in general. The number of authors and artists who are starting-up is proportionally small in comparison to the large number of copyright owners and industries. Online piracy more often decreases the profits of copyright owners rather than increase their reputations and popularity.

---

99. Barry Sookman & Dan Glover, *Graduated Response and Copyright: An Idea that is Right for the Times*, BARRY SOOKMAN (Jan. 20, 2012), http://www.barrysookman.com/2010/01/20/graduated-response-and-copyright-an-idea-that-is-right-for-the-times/.

100. Haber, *supra* note 89.

101. *Id*.

### C. *Impacts on Internet Service Providers*

The graduated response system can prevent ISPs from being sued for indirect infringement by establishing cooperation between copyright owners and ISPs. Upon satisfying the requirements of sending internet users warnings and disconnecting internet access, ISPs will not be held indirectly liable for the infringing activity of internet users. Thus, the graduated response system saves time, labor and costs for ISPs in otherwise dealing with civil lawsuits. ISPs have more resources to improve and maintain their services without concern about being scapegoats for infringing activity.[102] In this regard, the graduated response system plays a similar role as the safe harbor rules regulated by Section 512 of the DMCA. In addition, the graduated response system can help ISPs to resolve the problem of network traffic and congestion.[103] Since rampant online file-sharing results in limited bandwidth, network congestion and declining quality of user experience, disconnection of internet access of infringing users can restore network flow and the quality of overall user experience. Prior to the enactment of the graduated response policy, ISPs had to monitor their subscribers in order to improve the quality of services. Deep packet monitoring may cause ISP to identify the nature and type of traffic and actual knowledge of infringement by subscribers, and thus, will render ISPs ineligible from safe harbor protection.[104]

However, these advantages for ISPs are likely to be outweighed by the high expenses that they need to pay for the implementation of a graduated response system. In order to ensure the functionality of a graduated response system, ISPs must invest in surveillance, identification of subscribers, sending notifications of alleged infringement, running call centers to answer questions, developing new equipment to manage the system, maintaining data retention and reallocating human resources.[105] These expenses will be much higher than the subscription fees that internet users pay to the ISPs. Increase of subscription fees will negatively affect both the ISPs and internet users. Moreover, the graduated response system may put ISPs into another dilemma: satisfying complaints from copyright owners by warning alleged internet users and disconnecting internet access without further investigation will reduce user experience and put ISPs at risk of losing customers.

---

102. Yu, *supra* note 87.

103. Yu, *supra* note 87.

104. Rob Frieden, *Internet Packet Sniffing and Its Impact on the Network Neutrality Debate and the Balance of Power between Intellectual Property Creators and Consumers*, 18 FORDHAM INTELL. PROP. MEDIA & ENT. L.J. 633 (2008).

105. Michael Geist, *Estimating the Cost of a Three-Strikes and You're out System*, MICHAEL GEIST (Jan. 26, 2010), http://www.michaelgeist.ca/content/view/4731/135; Yu, *supra* note 87; Haber, *supra* note 89.

However, further investigation on determining the real activity of suspected internet users will increase their costs and possibly render them ineligible for safe harbor protection provided by current copyright statutes.

In summary, the disadvantages brought on by a graduated response system to ISPs very likely outweigh the advantages, because the expenses that ISPs will spend on the implementation of the new system may offset or even exceed those that they spend on litigations. Although the graduated response system can maintain network flow, and thus the quality of services, the effective implementation of such a system will put ISPs at risk of losing customers, which is a greater issue if ISPs profit from internet users.

### D. *Impacts on Internet Users*

Compared with being sued by powerful copyright industries and facing unfair judgment, internet users will feel that the graduated response policy is a better approach to sanction online copyright infringement and the outcome of such a policy is more acceptable than a large amount of compensation or imprisonment. Prior to the release of the graduated response system, the courts reached quite a number of judgments that heavily awarded the copyright industries for damage, and against individual online file-sharers, which aroused public concern on the fairness between damage and harm caused by file-sharing to copyright owners. In the judgments, a woman was fined 54,000 USD for infringing 24 songs;[106] a man in Hong Kong was sentenced to three-months of imprisonment for uploading three movies by using BitTorrent;[107] and another man was sentenced to jail for eighteen months in the United States for copyright infringement by using peer-to-peer file sharing technology.[108] Disconnection from the internet as stipulated by the graduated response system seems to be more agreeable to internet users than the remedies in civil and criminal litigations. Besides replacing severe remedies, the improvement of network flow as a result of the graduated response system can also benefit internet users, especially those who never or hardly infringe copyright.

Despite their relative advantages, the graduated response system has serious negative impacts on a series of fundamental rights of internet users,

---

106. Capitol Records, Inc. v. Thomas-Rasset, Memorandum of Law & Order, Civil File No. 06-1497 (MJD/LIB), document 457 (D. Minn. 2011) ; *Capitol v. Thomas*, WIKIPEDIA, http://en.wikipedia.org/wiki/Capitol_v._Thomas (last visited Sept. 7, 2011). The first trial in 2007 ordered the defendant to pay $222,000 in statutory damages. The second trial in 2009 ordered $1,920,000 in statutory damages and later reduced the amount to $54,000. The third trial in 2010 resulted in an award of $1.5 million and was reduced by court in July 2011 to $54,000 or $2,250 per song.

107. Chan Nai Ming v. HKSAR [2007] 10 H.K.C.F.A.R. 273 (C.F.A.).

108. United States v. Dove 585 F. Supp. 2d 865 (W. Va. 2008).

including the right of due process, freedom of expression and right of privacy. In addition, the graduated response system may not satisfy the requirements for fairness in legal enforcement and may disrupt the balance of interests between copyright owners and public users.

First, the graduated response system deprives internet users of due process due to the lack of verification on their suspected infringing activity. Since the complaints from copyright owners are generated by third-party companies that rely on automated web technologies and databases of digital fingerprints, alleged infringing activity will not be investigated by either the copyright owners or ISPs.[109] The detection process of infringement based on unreliable automatic-identification technology has been proven "notoriously inaccurate" through various cases which imposed sanctions on people who do not have computers or are deceased.[110] Even though technology can be improved to improve accuracy, large copyright industries such as records and motion picture companies are inclined to outsource the task of searching for suspected infringement to third-parties which are financially motivated to send as many notices as possible.[111] If tried under judicial procedures, these alleged infringers may be proven innocent based on defenses such as fair use or errors, and may be compensated if there are losses due to being wrongfully identified. However, the judicial verification and remedy process will not appear in a graduated response system which is enforced by private parties rather than judicial authorities. Copyright owners are not likely to carefully screen the suspected infringers, as their copyright works will be better protected if more end-users are deterred from committing infringement. Neither will ISPs examine the facts in case they lose their current safe harbor protection. Without the inclusion of due process, internet users cannot guarantee certain procedural rights, such as the right to be heard in a trial and the right to have their complaints fully considered by courts or a neutral judge.[112] Although the French policy allows internet users to be heard by the HADOPI, such procedure cannot fully meet the standards of due process due to the administrative nature of the HADOPI.

Secondly, the graduated response system may suffocate the freedom of expression and speech by intimidating internet users by cutting off their access to the internet which has already become a very important communication channel in everyday life. The freedom of expression and speech is a basic human right that includes "freedom to hold opinions without interference and to seek, receive and impart information and ideas

109. WILLIAM PATRY, MORAL PAMICS AND THE COPYRIGHT WARS 13 (2009).
110. *Id*.
111. PATRY, *supra* note 109, at 17.
112. Haber, *supra* note 89.

through any media and regardless of frontier".[113] With the development of digital network technology, the internet has become a major medium that facilitates access to information, publishing of expressions or artistic works via digital books and journals, blogs, online chatting forums or podcasting as well as personal interaction through email or instant messaging services. Internet surfers will largely reduce their online communications due to the threat of internet disconnection for fear that their thoughts and expressions would be monitored and consequently, suppress their thoughts.

Thirdly, the graduated response system may undermine individual internet privacy by imposing ISPs to monitor and retain the identity and relevant data of alleged repeat infringers. Personal data under the digital network environment including IP addresses and information about the activities linked to such addresses are usually anonymous. Upon finding suspected infringing activity, copyright owners will release the identity of alleged infringers to ISPs, thus giving intermediaries knowledge on previously anonymous personal data of the subscribers. In order to recognize repeat infringers, ISPs will retain such personal data for a long period of time or even exchange data with other ISPs in case they are not able to accomplish the task after receiving second or third notifications from copyright owners. Such data retention or exchange can jeopardize personal privacy because of the monitoring and preservation of information with regard to individual behaviors of users and activities carried out by private parties.

Finally, the graduated response system may lead to disproportion and imbalance in copyright systems by strengthening the power of copyright owners in addressing infringement against the interests of end-users in acquiring information, recreation and free expression. As Professor Peter Yu indicated, "taking away an individual's Internet access as a penalty for alleged copyright infringement is even worse than introducing criminal sanctions for downloading and peer-to-peer file sharing. While the criminal court system will determine whether sanctions will attach under the 'beyond a reasonable doubt' standard, a graduated response system may involve mere allegations of infringement of copyright holders or their industry group."[114] The "mere allegations of infringement" also discourage opportunities for users to provide a fair use or fair dealing defense. Even downloading material for non-commercial research purposes or file-sharing user-generated contents is likely to be deemed as infringement and punished by network disconnection. Some users may stop legal use after receiving the first or second warnings due to a lack of intellectual property knowledge.

113. Universal Declaration of Human Rights, G.A. Res. 217(III)A, U.N. Doc. A/RES/217(III), art. 19 (Dec. 10, 1948).

114. Yu, *supra* note 87, at 1401.

Both erroneous accusations by copyright owners and the misunderstanding of the users themselves will seriously narrow the scope of privileges that were originally enjoyed by the users.

To conclude on the impacts of the graduated response system on internet users, the negative factors strongly outweighs the relatively positive factors. The protection of the right of due process, freedom of expression and right of privacy as well as maintaining a balance of interest against copyright owners is more important to internet users than the enjoyment of quality network services or avoiding unfair judgments. After all, few users need to pay copyright owners large statutory damages or are criminalized and imprisoned because of unfair judgments, but quite a number of consumers will be disconnected from internet access, thus facing the risk of losing privacy, free speech and due process under the graduated response system.

### E. *China's Reaction to the Graduated Response System*

The graduated response system has not aroused public concern in China yet. The only public discussion on the new system reported by the news is a conference held by the copyright administrative organ of the Hebei Province in March 2011.[115] In this conference, experts from legislatures, administrative organs, industries and the academia discussed the strengthening of copyright protection in the digital network environment and promoting the development of content industries. The graduated response system was introduced and supported by scholars in this conference to better inhibit online copyright infringement and piracy. However, until now, there has not been any response from the state authorities on whether China should adopt the graduated response system.

Supporters of the graduated response system may argue that China is a country where copyright infringement is severe. Due to the large number of population and internet users, the enforcement of copyright protection in the digital network environment will be quite difficult in China. Traditional copyright protection is based on licensing by copyright owners or authorized proxies, while users in the digital environment can easily obtain works through digital network technologies. The quick development of cloud computing technology which aims to achieve a unified management and scheduling of network resources further aggravates the difficulties of

115. *Hê,ho Pei Fên Chieh Tuan Hsiang Ying Ts'o Shih Huo K'ê I Chih Wang Lao Ch'in Ch'üan Tao Pan* [*Hebei: the Graduated Response System May Inhibit Online Infringement and Piracy*], CHUNG HUA JÊN MIN KUNG HAN KUO KUO CHIA CHIH SHIH CH'AN CH'ÜAN CHÜ [STATE INTELLECTUAL PROPERTY OFFICE OF P.R.C.], http://www.sipo.gov.cn/wqyz/dfxx/201104/t20110407_595456.html (last visited Sept. 7, 2011).

copyright protection enforcement.[116] Moreover, due to the previous absence of strong governmental execution and general education on intellectual property law, a culture that respects intellectual property rights has not yet been well formed in China. The importation of the graduated response system may help to effectively address copyright infringement and educate people to respect copyrights.

Opponents of the graduated response system may focus on the disadvantages discussed above to argue that China has already adopted a strict network filtering policy and should not further intensify network control. According to a filtering watchdog group, the Open Net Initiative, "China has one of the largest and most sophisticated filtering systems in the world".[117] By establishing a complex system of regulation, licensing and ISP liability, China can control internet usage and touch every point of internet access and transmission.[118] The introduction of a graduated response system will exacerbate the current situation. Under certain circumstances, the government may exploit the graduated response system to disconnect linkage to the internet for public administration purposes rather than merely for copyright protection. Taking freedom of expression, due process and privacy issues into consideration, China should not rashly import the graduated response policy without carefully examining whether the advantages will outweigh the disadvantages in the national situation. It is better for China to wait and observe the effect of the graduated response system that has been implemented in overseas jurisdictions and then to decide whether she should import the new policy.

Even if China intends to transplant the graduated response system to address digital copyright infringement, in the face of pressure from protecting copyright industries and maintaining an international image, several factors should be seriously considered in the establishment of such a new system. These factors are proposed by Professor Peter Yu, which include the introduction of "independent review" mechanisms which will avoid the wrongful identification of suspected infringers as much as possible through judicial or administrative processes; system's "educative and rehabilitative" purposes under which internet users should easily understand the contents of the warnings and the reason why their actions are wrong;

---

116. *Wang Lo Shih Tai PanCh'üanPao HuHsien ChuangTiaoCh'a: Chü ChengTse JenKuo ChungChih WeiCh'üan Nan* [*Investigation of Status Quo of Copyright Protection in the Network Age: Severe Burden of Proof Makes Protection of Rights Difficult*], CHUNG KUO CHING CHI WANG [CHINA ECONOMIC NET], (Apr. 1, 2011), http://www.ce.cn/xwzx/gnsz/gdxw/201104/01/t20110401_22340359_1.shtml.

117. Jim Burger, *ANALYSIS: Filtering & Graduated Response against Online Infringers*, DVD-AND-BEYOND (Sept. 26, 2010), http://www.dvd-intelligence.com/features/feature.php?feature=71.

118. *Id*.

maintaining of "reasonable alternative access" to the internet; minimization of "collateral damages"; safeguarding of "proportionality" so that protection of copyright interests would not damage the protection of free speech and privacy, and "flexibility" so that alleged infringers could claim a fair use defense or lack of originality of copyright ownership; and finally, the use of "internet disconnection as a last resort" if less severe measures such as "bandwidth reduction, monitored access, or site, port, or protocol blocking" are available.[119]

## VI. CONCLUSION: RECOMMENDATIONS FOR ESTABLISHING CERTAINTY OF INTERNET SERVICE PROVIDER LIABILITY

Currently, China has been launching the third revision to the Copyright Law and widely seeking public opinions. The National Copyright Administration of China (NCAC) released the first Draft Amendment to the Copyright Law and the Brief Explanations on the Draft Amendment on 31 March 2012, and the second Draft Amendment and the Brief Explanations on 6 July 2012. The third Draft Amendment based on the previous two drafts and relevant public opinions was concluded in October 2012 and ready for submission to the Standing Committee of the People's Congress for final review and promulgation. As opposed to the previous two revisions that were propelled by external pressures, the third revision is the response to China's national intellectual property strategy to build up an innovative country and with the purpose to make the Copyright Law completely adaptive to the digital network environment.

In the new round of reform in China, only one provision in the Draft Amendments relates to ISP liability and safe harbor. Article 69 of the Draft Amendments is concerning the indirect liability and safe harbor for copyright infringement committed by ISPs. It separates ISPs from internet content providers (ICPs) via immunizing ISPs' investigation responsibility if such ISPs merely offer internet users pure network technical services such as storage, searching, linking, *et cetera*. ICPs which provide works, performance or sound recordings via information network cannot be immunized from such liability.

Article 69 further incorporates three principles: notice and takedown procedure, red flag standard and contributory liability. Under the notice and takedown procedure, upon receiving notice from copyright owners who require taking necessary measures to attack alleged copyright infringement, such as deleting, shielding or blocking the hyperlink to the infringing work, ISPs should immediately take actions. Otherwise, they may be held liable for

119. Yu, *supra* note 87, at 1419-29.

infringement conducted by their subscribers.

Under the red flag standard, ISPs will be held liable for indirect infringement if they know or should know the existing copyright infringement on their network and do not take immediate and necessary measures against the infringement. The constructive knowledge of ISPs is explained by the Circular on Issuing the Guiding Opinions on the Protection of the Right of Communication through Information Network (Trial Implementation) issued by the Beijing Municipal Bureau of Copyright which stipulates that repeated uploading by subscribers of infringed works which have been required to be deleted shall illustrate obviousness of the infringement.[120]

Under contributory liability, ISPs will be held liable if they instigate or aid others to commit infringement of copyright. Potential instigation or aiding activities are indicated by some case decisions,[121] including offering search engine and software for subscribers to search and download copyright works, or advertising on the website to attract the public to become subscribers for free enjoyment of copyright works.

Differing from protection of technological measures and digital rights management information which is stipulated under a specific chapter, provisions regarding ISP liability and safe harbor are too simplified and abstract to embody the important categories of liability immunization, key factors gauging liability and detailed procedures concerning the notice and takedown regime. Lacking in the specified stipulations already offered by the 2006 Regulation, the ISP liability and safe harbor provision in the Draft Amendments can be deemed as retrogression.

Based on the review and analysis of the development of ISP liability and safe harbor regulation among different jurisdictions, several suggestions are made for establishing the certainty of ISP liability in general and for China's digital copyright reform on ISP liability in particular.

First, certain standards about the following factors should be settled either in common law indirect liability principles or statutory liability regulations of ISPs: the knowledge of ISPs on primary infringement, the obtaining of direct financial benefits from primary infringement and the ability to control or supervise infringing activity. In summary, in terms of the

120. The Guiding Opinions on the Protection of the Right of Communication through Information Network (Trial Implementation) (formulated by the Beijing Municipal Bureau of Copyright, May 10, 2011, effective Aug. 1, 2011), art. 5: "Network service providers who provide information storage space to service clients shall stop any service clients who repeatedly upload the works of other people without permission. If the interference by the providers fails to produce effect, services provided to them shall be terminated and the same shall be reported to the copyright administrative enforcement authority."

121. *See, e.g.*, *Shang Hai P'an Li Chiao So Wang Min Ch'in* [*The First Case on Soliciting and Aiding Netizens Infringement in Shenghai*], HSIN HUA WANG [NEWS] (Nov. 23, 2011), http://news.xinhuanet.com/legal/2007-11/23/content_7132641.htm.

first factor, ISP knowledge shall include both actual knowledge and awareness of apparent infringing activity. The emergence of certain situations should be deemed as apparent infringing activity, including abnormally high traffic on the network, the appearance of terms like "pirated" or "bootleg" in the file title, inclusion of names of copyright works in the file title of which the uploader is obviously not the copyright owner, and the repeated appearance of materials that have been targeted by statutory takedown notices. However, mere knowledge of the prevalence of infringing activity in general should not be deemed as awareness of apparent infringement. As for the second factor, direct financial benefits should show a very close relationship between ISPs and the alleged infringing activity. Situations such as the attraction of advertising probably by the popularity of the infringing material shall not be deemed adequate to prove a close relationship between an ISP and the alleged infringer. As for the third factor, the ability to control or supervise subscriber activities could mean that ISPs' prerequisite ability to intervene in the infringing activities.

Secondly, the design of immediate takedown requirements in the notice and takedown regime increases the risk of erroneous takedowns. The notice and takedown regime can be reformed in a stepwise manner by incorporating a reasonable grace period for suspected subscribers to defend themselves, and the establishment of certain exemptions by ISPs even if they fail to take down the suspected infringing material. In the first step, a reasonable grace period can be incorporated for suspected subscribers to defend themselves prior to the removal of their material by ISPs. A reasonable grace period could be around four to five days which is neither too short for subscribers to prove their innocence nor too long for copyright holder and ISPs to monitor the suspected subscribers and address the infringement. Under circumstances in which the suspected subscriber does not respond during the grace period after receiving a notice from the ISP, the ISP should expeditiously take down the material in case they are deemed to be liable for the infringement. The period of time within the expeditious takedown should be better defined as twenty-four hours. In the second step, some exceptions can be established in the grace period, including special circumstances under which ISPs can immediately take down the suspected material without waiting for the end of the grace period. Examples include the circumstances where copyright owners have already suffered great losses due to the unauthorized online transmission of their works. In the third step, special exemptions can be established, which still allow ISPs to be protected by safe harbors even if they fail to take down the suspected material after the notice and the grace period. Such exemptions include circumstances where enforcement of the takedown will cause great economic loss or impose undue burden on the ISPs. In China's situation, the counter notification procedure should be

maintained. The combination of "notice and takedown with a grace period" and "counter notification" will better achieve the multiple purposes of controlling digital copyright infringement, promoting ISP participation in online information dissemination and e-commerce, and protecting the interests of internet consumers.

Thirdly, China does not include a "subpoena procedure" as found in the United States or the "Norwich Pharmacal" discovery procedure as found in Hong Kong. Instead, the administrative organ in China is allowed to disclose the personal information of subscribers. Although the administrative approach is more efficient and coercive than any other measure, the protection of the privacy of subscribers is more at risk due to the high possibility of administrative power abuse. It is understandable that the adoption of administrative procedures in information collection by the Chinese government aims to effectively supervise the suspected infringers and resolve the rampant piracy problem in China. However, the privacy of subscribers may be seriously infringed if the alleged infringer is finally proven to be innocent. The aforementioned comparative discussion between the "subpoena procedure" and "Norwich Pharmacal" discovery procedure shows that the latter places more concern on the protection of privacy because of the prerequisite in which a person who is seeking for a court order should have a genuine intent to commence a proceeding. Therefore, China could consider importing the "Norwich Pharmacal" procedure to balance the interests of different parties. On the one hand, China could grant the authority to district or intermediate courts to decide whether the information of the alleged infringers should be disclosed upon the requests made by copyright holders. On the other hand, Chinese legislations could include a provision that requires ISPs to record the information of suspected infringers when a judicial procedure is commenced.

Fourthly, China should not rush to adopt a graduated response policy without carefully examining and balancing the positive and negative factors that will impact copyright owners, ISPs and internet users. Even if the Chinese government intends to adopt the graduated response system, several key factors should be taken into consideration as mentioned above: an "independent review" mechanism, "educative and rehabilitative" purposes, the maintaining of "reasonable alternative access" to the internet; minimization of "collateral damages"; safeguarding of "proportionality" and "flexibility", and the use of "internet disconnection as a last resort".

Finally, China should adopt heterogeneous approaches combined with legislative measures to better achieve the certainty of ISP liability and the free flow of information. In addition to revisions to current copyright laws and regulations, China should broadly adopt various other methods, including revision of other relevant laws such as competition and privacy

laws, government policy and industry guidelines, as well as introduction of public consultation and multi-party forums so as to make these mechanisms collaboratively work on the issues of ISP liability, free dissemination of information, and protection of privacy in the digital network environment. Hong Kong has already set a good example for Mainland China by collecting opinions and comments from different stakeholders via public consultations and drafting proposals for legal reforms. In December 2006, the Hong Kong government issued a public consultation document to seek opinions from various sources on how copyright protection should be strengthened in the digital age.[122] After the public consultation, the Hong Kong government released the Preliminary Proposals for Strengthening Copyright Protection in the Digital Environment for further public engagement in April 2008.[123] After further public consultations were held in 2008 and at the Tripartite Forum, the Hong Kong government released the Proposals for Strengthening Copyright Protection in the Digital Environment in 2009 as a reference source for legal reform.[124] Mainland China may thus learn from Hong Kong to obtain more feedback from the public so as to create more realistic and reliable copyright reform proposals. When applying heterogeneous approaches to digital legal reforms, it is important for China to avoid potential overlapping and conflicts between different approaches and try to merge them so that they are able to systematically and consistently resolve legal issues under the digital network environment.

122. *Consultation on Copyright Protection in the Digital Environment*, H. K. INTEL. PROP. DEPT. (Dec., 2006), http://www.info.gov.hk/archive/consult/2007/digital_copyright_e.pdf.

123. *Supra* note 82.

124. *Supra* note 98.

## REFERENCES

17 U.S.C. § 512 (2010).

35 U.S.C. § 271 (2010).

A&M Records Inc. v. Napster Inc., 239 F.3d 1004 (9th Cir. 2001).

WIPO (1996). *Agreed Statements Concerning the WIPO Copyright Treaty, concerning article 8*. Retrieved from http://www.wipo.int/treaties/en/text.jsp?file_id=295456.

Anti-Counterfeiting Trade Agreement (2011). Retrieved from http://www.mofa.go.jp/policy/economy/i_property/pdfs/acta1105_en.pdf.

*Australia Copyright (Digital Agenda) Amendment Act 2000* (Cth) s 36(1A) (Austl.).

*Australian Tape Manufacturers Ltd. v Commonwealth of Australia* (1993) 25 IPR 1 (Austl.).

Brief for Deirdre K. Mulligan, as Amici Curiae Supporting Reversal, Stephen J. Barrett M.D., et al. v. Ilena Rosenthal, 51 Cal.Rptr.3d 55 (2006) (No. S122953). Retrieved from https://www.eff.org/sites/default/files/filenode/Barrett_v_Rosenthal/law_professors_amicus_brief.pdf.

Burger, J. (2010, September 26). ANALYSIS: Filtering & graduated response against online infringers. *DVD and beyond*. Retrieved from http://www.dvd-and-beyond.com/display-article.php?article=1378.

Capitol Records, Inc. v. Thomas-Rasset, Memorandum of Law & Order, civil file No. 06-1497 (MJD/LIB), document 457 (D. Minn. 2011).

Chan Nai Ming v. HKSAR [2007] 10 H.K.C.F.A.R. 273 (C.F.A.).

China Internet Network Information Center (2001). Semiannual survey report on development of China's internet. Retrieved from http://www.cnnic.net.cn/download/manual/en-reports/7.pdf.

China Internet Network Information Center (2006). 17th statistical survey report on the internet development in China. Retrieved from http://www.cnic.cas.cn/qkbg/cnnictjbg/cnnictjfz/200601/P020090819615860278077.pdf.

China Internet Network Information Center (2011). 28th statistical survey report on the internet development in China. Retrieved from http://www1.cnnic.cn/IDR/ReportDownloads/201209/P020120904421102801754.pdf.

Chisum, D. S. (2004). *Chisum on Patents* (Vol. 5). New York, NY: LexisNexis.

Chung Kuo Yin Lê Chao Tso Ch'üan Hsieh Hui v. Wang I Kung Ssu & I Tung T'ung Shên Kung Ssu [Music Copyright Society of China (MCSC) v. Guangzhou NetEase Computer System Inc. & China Mobile Beijing Co., Ltd.] (Beijing 2d. Interm. People's Ct. Sept. 20, 2002) (Westlaw China).

Dish Network LLC & Others v. Zentek International Co. Ltd. & Another [2009] H.K.E.C. 220. Retrieved from http://m.hg.org/law-articles/area-intellectual-property/7729/IP_Law_%E2%80%93_Application_for_Norwich_Pharmacal_Relief.

Explanatory Memorandum, Copyright Amendment (Digital Agenda) Bill 1999 (Cth) (Austl.).

Falcon v. Famous Players Film Co. Ltd., [1926] 2 K.B. 474.

Frieden, R. (2008). Internet packet sniffing and its impact on the network neutrality debate and the balance of power between intellectual property creators and consumers. *Fordham Intellectual Property, Media and Entertainment Law Journal, 18*, 633-675.

Geist M. (2010, January 26). Estimating the cost of a three-strikes and you're out system [Web log post]. Retrieved from http://www.michaelgeist.ca/content/view/4731/135.

Ginsburg, J. & Ricketson, S. (2006). Inducers and authorisers: A comparison of the US Supreme Court's Grokster decision and the Australian Federal Court's KaZaa ruling, *Media and Arts Law Review, 11*, 1-25.

Ginsburg, J. C. (2010). User-generated content sites and section 512 of the US Copyright Act. In I. A. Stamatoudi (Ed.), *Copyright enforcement and the internet*. (pp. 183-300). The Netherlands: Kluwer Law International.

Haber, E. (2010). The French revolution 2.0: Copyright and the three strikes policy. *Journal of Sports and Entertainment Law, 2*, 297-339.

*Hê,ho Pei Fên Chieh Tuan Hsiang Ying Ts'o Shih Huo K'ê I Chih Wang Lao Ch'in Ch'üan Tao Pan* [*Hebei: the Graduated Response System May Inhibit Online Infringement and Piracy*], CHUNG HUA JÊN MIN KUNG HAN KUO KUO CHIA CHIH SHIH CH'AN CH'ÜAN CHÜ [STATE INTELLECTUAL PROPERTY OFFICE OF P.R.C.]. Retrieved from http://www.sipo.gov.cn/wqyz/dfxx/201104/t20110407_595456.htm

Hong Kong Commerce & Economic Development Bureau (2008a, April). Preliminary proposals for strengthening copyright protection in the digital environment. Retrieved from http://www.ipd.gov.hk/eng/intellectual_property/copyright/Consultation_Document_Prelim_Proposals_Eng%28full%29.pdf.

Hong Kong Commerce & Economic Development Bureau (2008b, April). Proposals for strengthening copyright protection in the digital environment. Retrieved from http://www.legco.gov.hk/yr09-10/english/panels/ci/papers/ci1117cb1-341-8-e.pdf.

Hong Kong Intellectual Property Department (2006, December). Consultation on copyright protection in the digital environment. Retrieved from http://www.info.gov.hk/archive/consult/2007/digital_copyright_e.pdf.

In re Aimster Copyright Litigation 334 F.3d 643 (7th Cir. 2003). Metro-Goldwyn-Mayer Studios Inc. v. Grokster Ltd., 380 F.3d 1154 (9th Cir. 2004).

Metro-Goldwyn-Mayer Studios Inc. v. Grokster Ltd., 545 U.S. 913 (2005).

Meyer, D. (2010, January 26). Europe 'will not accept' three strikes in ACTA treaty. *ZDNet*. Retrieved from http://www.zdnet.co.uk/news/networking/2010/02/26/europe-will-not-accept-three-strikes-in-acta-treaty-40057434/.

*Opinion of the European Data Protection Supervisor on the current negotiations by the European Union of an Anti-Counterfeiting Trade Agreement (ACTA)*, 2010 O.J. (C147)1 ¶¶ 21 & 22. Retrieved from http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2010/10-02-22_ACTA_EN.pdf.

Patry W. (2009). *Moral panics and the copyright wars*. New York, NY: Oxford University Press.

Practical Law (n.d.). *Norwich Pharmacal orders: A quick guide*. Retrieved from http://ld.practicallaw.com/0-211-3137.RCA Corp v. John Fairfax & Sons Ltd., [1982] R.P.C. 91.

Shang Hai P'an Li Chiao So Wang Min Ch'in [The First Case on Soliciting and Aiding Netizens Infringement in Shenghai]. (2011, November). *Hsin Hua Wang* [*News*]. Retrieved from http://news.xinhuanet.com/legal/2007-11/23/content_7132641.htm.

Shên Hsi Wang Lao Ch'uan Po Ch'üan Pao Hu T'iao Li [Regulation on the Protection of the Right to Network Dissemination of Information] (promulgated by the St. Council, May 10, 2006, effective July 1, 2006), art.13-16; 20-25. (China).

Sony Corp. of America v. Universal City Studios, Inc., 464 U.S. 417 (1984).

Sookman, B. & Glover, D. (2010, January 20). Graduated response and copyright: An idea that is right for the times [Web log post]. Retrieved from

http://www.barrysookman.com/2010/01/20/graduated-response-and-copyright-an-idea-that-is-right-for-the-times/.

Universal Declaration of Human Rights, G.A. Res. 217(III) A, U.N. Doc. A/RES/217(III), art. 19 (December 10, 1948).

United States v. Dove 585 F. Supp. 2d 865, (W. D. Va. 2008).

Universal City Studios, Inc. v. Sony Corp. of America, 659 F.2d 963 (9th Cir. 1981)

University of New South Wales v. Moorhouse 133 CLR 1 (1975). U.S. Copyright Office (1998, December). The Digital Millennium Copyright Act of 1998: U.S. Copyright Office Summary. Retrieved from http://www.copyright.gov/legislation/dmca.pdf.

Viacom Intern. Inc. v. YouTube, Inc., 718 F.Supp.2d 514 (2010).

Wang Lo Shih Tai PanCh'üanPao HuHsien ChuangTiaoCh'a: Chü ChengTse JenKuo ChungChih WeiCh'üan Nan [Investigation of Status Quo of Copyright Protection in the Network Age: Severe Burden of Proof Makes Protection of Rights Difficult]. (2011, April 1). *Chung Kuo Ching Chi Wang* [*CHINA ECONOMIC NET*]. Retrieved from http://www.ce.cn/xwzx/gnsz/gdxw/201104/01/t20110401_22340359_1.shtml.

*WEA International Inc. v Hanimex Corporation Ltd*. (1987) 10 IPR 349 (Austl.).

Weinberg M. (2010, February 1). Three strikes, exile, and Judge Dredd. *Public Knowledge*. Retrieved from http://www.publicknowledge.org/node/2877.

Wikipedia (n.d.). *Capitol v. Thomas*. Retrieved from http://en.wikipedia.org/wiki/Capitol_v._Thomas.

Wikipedia (n.d.). *Graduate Response*. Retrieved from http://en.wikipedia.org/wiki/Graduated_response.

WIPO Copyright Treaty, art. 8. Dec. 20, 1996, 2186 U.N.T.S. 121.

Workman S. W. (2008, August 24). Internet law-developments in ISP liability in Europe. *Internet Business Law Services*. Retrieved from http://www.ibls.com/internet_law_news_portal_view.aspx?id=2126&s=latestnews.

Yu, P. K. (2010). The graduated response. *Florida Law Review, 62*, 1373-1430.

# 建立網路服務提供者責任及安全港規則的確定性

華　劼

## 摘　要

為了回應國際條約中保護資訊網路傳播權的要求和打擊氾濫的網路盜版行為，不同司法管轄區的著作權相關法律和政策都開始對引誘或協助網路使用者侵權的網路服務提供者追究侵權責任。雖然由案例發展而來的安全港規則已經被吸收進立法，但其中的相關機制，例如「通知及取下」、「傳票程序」、「三振條款」等，仍會阻礙資訊傳播及侵犯個人隱私。

本文旨在建立網路服務提供者責任的確定性以及緩和不斷加強網路服務提供者責任的趨勢，並通過審視和分析不同司法管轄區之間關於網路服務提供者責任的著作權制度，為中國的數位著作權改革提供建議。本文第二部分將討論網路服務提供者的定義以及建立間接侵權責任確定性和可預測性的重要意義。本文第三部分將分析安全港規則、由美國法院判決發展而來的輔助及代理侵權責任、以及從英聯邦司法管轄區案例發展而來的授權及共同侵權責任。本文第四部分將審視有關網路服務提供者責任及其限制的法定要求。這部分主要討論美國、中國和香港的法律，因為這些司法管轄區的法律體現出一個相對完整的網路服務提供者責任制度。本文第五部分將會審視「三振條款」，該項措施是諸如法國等司法管轄區域的新發展，通過給安全港規則添加新條件來強化網路服務提供者的責任。本文第六部分將會建議調整有關網路服務提供者侵權責任的數位著作權法律，從而實現中國的數位著作權改革，並平衡著作權所有者、網路服務提供者、以及網路使用者之間的利益平衡，建立網路服務提供者責任的確定性。

**關鍵詞：網路服務提供者；間接侵權責任；安全港；利益平衡**