IIC (2015) 46:275–309
DOI 10.1007/s40319-015-0325-0

ARTICLE

# Development of Hosting ISPs' Secondary Liability for Primary Copyright Infringement in China – As Compared to the US and German Routes

**Jie Wang**

Published online: 21 April 2015


**Abstract** This article takes a comparative approach to studying the development of hosting ISPs' secondary liability in China, namely by referring to relevant rules in the US and Germany as examples. In particular, this article compares how the courts interpret the main imputed factors in these three jurisdictions such as monitoring responsibility, knowledge of infringement, measures against repeating infringement, benefit from infringement, and inducement. Through the aforesaid comparison, this article notes that the development of hosting ISPs' secondary liability in China has been deeply affected by the relevant rules in the US and Germany, but it is also marked with its own characteristics such as requiring the hosting ISP to exert a higher level of duty of care on hot-play films and television dramas, and famous works. Moreover, this comparison also reveals that although China, the US, and Germany mainly rely on different approaches to solve hosting ISPs' secondary liability, the recent case decisions in these three jurisdictions have shown some common tendencies, for example, receiving benefits has become a less important imputed factor, and the courts tend to pay more attention to hosting ISPs' intent and commercial model when deciding liability.

I would like to thank Prof. A.W.J. Kamperman Sanders for his supervision; Prof. Dr. Reto M. Hilty and Dr. Silke von Lewinski for their help in my study on hosting ISPs' secondary liability in Germany; and Prof. Llewellyn Gibbons and Prof. Lars S. Smith for the correction done by them. This paper was sponsored by the China-EU School of Law (CESL) at the China University of Political Science and Law (CUPL) http://www.cesl.edu.cn. The activities of CESL at CUPL are supported by the European Union and the People's Republic of China.

J. Wang (✉)
PhD Researcher, Faculty of Law, Maastricht University (Maastricht, The Netherlands); PhD Candidate, Center for Study of Intellectual Property Right, ZhongNan University of Economics and Law (Wuhan, China); Scholarship Holder, Max Planck Institute for Innovation and Competition (Munich, Germany)
Maastricht, The Netherlands
e-mail: jie.wang@maastrichtuniversity.nl

**Keywords** Hosting ISP · Knowledge of infringement · Repeating infringement · Benefit from infringement · Intent · Commercial model

## 1 Introduction

Since the People's Supreme Court in China promulgated its first Interpretation concerning solving copyright disputes over the Internet in 2000, several pieces of legislation have been passed to discourage Internet copyright infringement, including the "Regulation on the Protection of the Right to Network Dissemination of Information" (hereinafter "the Regulation") issued by the State Council in 2006 and the "Tort Law of China" ratified by the Standing Committee of the People's Congress in 2010. During the same period, the Interpretation promulgated by People's Supreme Court was revised several times to meet the need to regulate a hosting Internet service provider's (ISP) secondary liability. The latest Interpretation, which provides many detailed norms based on prior judicial accomplishments in China and uses relevant US and EU judicial decisions as important references, deserves attention. To some extent in the last 30 years, the development of Chinese IP law has been moved forward under pressure from the US, so that Chinese IP laws are unavoidably affected by US law, and the legislation regarding hosting ISPs' secondary liability is no exception to this norm. However, as a country with a civil law system (unlike the US, a common law country), Chinese judges are well trained in civil law rather than common law. Therefore, when deciding IP infringement cases, Chinese judges sometimes tend to interpret a rule stemming from common law with their knowledge and background, which is based in civil law. Such decision-making often results in turmoil in judicial practice. The application of rules regarding hosting ISPs' secondary liability in China is a typical example. Nevertheless, in an attempt to escape such turmoil, Chinese judges have successfully configured their own way of dealing with hosting ISPs' secondary liability, from which one can still see the shadow of relevant US and EU law, yet it is in a way distinctive to Chinese characteristics.

## 2 Monitoring Responsibility and General Knowledge of Infringements

The "no monitoring responsibility" clause in the Digital Millennium Copyright Act (DMCA) §512 can be seen as offering a major concession to ISPs, under which an ISP does not need to "monitor its service or affirmatively seek facts indicating infringing activity,"[1] and it also functions as the backbone of "safe harbor" provisions. Furthermore, the "no monitoring responsibility" is closely related to another concept "general knowledge of infringements", which means that an ISP can be deemed to know definitely that some of its users transmit infringing content through the Internet service it offers, but it does not know exactly what content is transmitted and which users are infringing. By deducing from "no monitoring

[1] 17 U.S.C. §512(m)(1).

responsibility", the general knowledge of infringements cannot be understood as imputed knowledge in the context of DMCA §512. This is because if an ISP should be liable for its general knowledge of copyright infringement, then it must monitor its Internet service to seek out infringers and to stop further copyright infringement, since it is highly likely its service is being used for purposes of copyright infringement. William Patry points out, "as a result of this lack of any obligation to be pro-active in seeking out possible infringements, service providers cannot be tagged for imputed knowledge where there are infringing materials and the service provider does not take steps to identify or monitor such material."Thus, the "no monitoring responsibility" clause functions as a significant limitation on imputed knowledge.[2] In the US, whether general knowledge of infringement would lead a third party who had sold neutral products to undertake secondary liability was settled in the famous *Sony Betamax* case, which established a liability standard called "substantial noninfringing use" by referring to the "staple article of commerce" patent law doctrine.[3] According to this standard, if a product is capable of substantial noninfringing uses, its distribution cannot result in contributory liability, unless the distributor fails to take corresponding actions once knowing about a specific instance of infringement.[4] This implies that a general knowledge of infringement alone will not result in secondary liability. From a legal perspective, the Internet service offered by ISPs is similar to the Betamax sold by Sony, both of which are capable of substantial noninfringing use, so the rationale embodied in *Sony Betamax* has also been merged into DMCA §512. In brief, because of the "no monitoring responsibility" clause, courts in the US always refuse to enforce secondary liability against ISPs when the claim against them is based purely on the grounds of their general knowledge of infringement. In the case of *Viacom v. YouTube*, the court reaffirmed this doctrine again and rejected the plaintiff's attempt to interpret the "red flag" standard as an indication basis to hold the ISP liable for its general knowledge of direct infringements.[5]

In the EU, the Directive on Electronic Commerce provides similar rules concerning ISPs' monitoring responsibility. Member States shall not impose a general obligation on providers, when providing the service covered by Arts. 12 (mere conduit), 13 (caching) and 14 (hosting), to monitor the information they "transmit or store, nor a general obligation actively to seek facts or circumstances indicating illegal activity."[6] As one of more important EU members, Germany transplants this provision into Sec. 7(2) Telemedia Act (Telemediengesetz). Therefore, German courts also follow the doctrine of "no monitoring liability", and thus conclude that the general knowledge of infringements does not qualify as imputed knowledge. For example, *Greatest Hits II* held that "generic knowledge of infringing use is insufficient to trigger liability."[7] In *Rapidshare II*, the Hamburg

[2] Patry (2009).

[3] *See Sony Corp. of America v. Universal City Studios, Inc*., 464 U.S. 417, 442 (1984).

[4] *Id*.

[5] *See Viacom International, Inc. v. YouTube, Inc.*, 676 F.3d 19, 30–31 (2nd Cir. 2012).

[6] Directive 2000/31/EC, Art. 15.

[7] Düsseldorf District Court, *Störerhaftung des Filesharing-Betreibers*, 2008 MMR 759 (quoting Barazza 2012).

Court of Appeal held that "infringing use was foreseeable and likely, but noted that unless the service provider willfully ignores it, specific knowledge is still required to impose contributory liability."[8]

In China, the People's Supreme Court had already used DMCA §512 as an important reference when it provided the first Interpretation regarding hosting ISPs' liability;[9] however, for unknown reasons it did not integrate a "no monitoring responsibility" clause, which is an essential provision in DMCA §512.[10] Six years later, unfortunately again, the Regulation, which includes a Chinese version of "safe harbor" provisions, still did not address an ISP's monitoring responsibility, and this loophole has resulted in confusion concerning this issue in judicial practice. For example, in the case *vale.com v. tudou.com*, the Shanghai First Intermediate People's court concluded that the defendant, a video-sharing website operator, definitely knew that some of the works being uploaded by its users were infringing, so the defendant should have monitored the content uploaded by its users in order to filter out infringing content.[11] By contrast, in another case, *Wangyajun v. Lingshida Tech*, the court affirmed that the defendant, as an Internet platform offering information storing space, faced a huge volume of uploaded content each day, so that it was unreasonable to impose monitoring responsibility on the ISP.[12]

With the studies on ISPs' secondary liability arising in China, especially after many judicial decisions in the EU and US have been introduced into China, a consensus of no monitoring responsibility has been gradually reached in China. As stated by an official, ISPs have no obligation to monitor overwhelming amounts of content on the Internet and then decide whether it is infringing or not.[13] In 2012, the National Copyright Administration in China published two revised drafts of the proposed Copyright Law, both of which include an article which clearly states that if an ISP offers storage, search, linking or other purely technical services to Internet users, then it is not obliged to monitor the information concerning copyright or related rights.[14] Furthermore, the recently promulgated Interpretation also provides that where an ISP does not take the initiative to monitor Internet users' infringement of the right to network dissemination of information, the

[8] Hamburg Court of Appeal, *Haftung eines Sharehosting-Dienstes für rechtsverletzende Inhalte – Rapidshare II*, 2012 GRUR-RR 335, (quoting *Id*).

[9] *See* The Interpretation of the Supreme People's Court on Several Issues Concerning Application of Law in the Trial of Cases involving disputes about Infringing Right to Internet dissemination of information (2000), this Interpretation brought in "notice-delete" mechanism and subpoena calling for information to identify infringer from DMCA 512.

[10] *Id*, the Interpretation did not address the issue of an ISP's monitoring responsibility.

[11] *vale.com v. tudou.com*, No. 19 Hu Yi Zhong Min Wu (Zhi) ZhongZi (2009).

[12] *See Wangyajun v. Lingshida Tech*., No. 2775 Hai Min Chu Zi (2008).

[13] This statement was presented at a press conference on introducing "The Provisions of the Supreme People's Court on Several Issues Concerning Application of Law in the Trial of Cases Involving Disputes about Infringing Right to Internet Dissemination of Information (2013)" when the official was questioned about "ISPs' monitoring liability", (15 October 2013). http://www.sipo.gov.cn/mtjj/2013/201301/t20130121_783586.html.

[14] People's Republic of China Copyright Law (first revising draft), Art. 69, published by National Copyright Office in March 2012. In second revising draft, the same norm is also provided in Art. 69.

People's courts shall not conclude that it is at fault for allowing primary infringement to occur.[15] Since then, it has been officially rejected that the ISPs' general knowledge of primary copyright infringement can result in secondary liability, thus Chinese jurisdictions have begun to conform to prevailing practices in the US and Germany in this respect.

## 3 Specific Knowledge of Infringements

Specific knowledge is a concept related to general knowledge but with a different meaning from the legal perspective. As its name implies, unlike general knowledge, specific knowledge requires more than having a general awareness that infringements are occurring, but rather a precise knowledge that a particular incidence of infringement has occurred. The US, EU and China, all recognize that if an ISP possesses specific knowledge of infringement but does not expeditiously stop it, then it should be secondarily liable for these acts of infringements. As provided in the DMCA §512(c)(1)(A), in order to avoid monetary damages, the hosting ISP shall not.

> have actual knowledge that the material or an activity using the material on the system or Internet is infringing; in the absence of such actual knowledge, is not aware of facts or circumstances from which infringing activity is apparent; or upon obtaining such knowledge or awareness, acts expeditiously to remove or disable access to the material.[16]

The relevant provision in the EU Directive on electric commerce is quite similar to the DMCA provision. The EU Directive provides that if the hosting ISP does not "have actual knowledge of illegal activity or information and, as regards claims for damages, is not aware of facts or circumstances from which the illegal activity or information is apparent; and upon obtaining such knowledge or awareness, acts expeditiously to remove or disable access to the information."[17] In Germany, this provision has been incorporated into the Telemedia Act.[18] In China, the knowledge requirement for ISP liability immunity is articulated slightly differently from the provisions in the US and EU, and it reads as follows: "the (hosting) ISP has no knowledge of and no justifiable reason to know the infringement of the works, performance, sound or video recordings."[19] From the above provisions, it is clear that "specific knowledge" can be categorized into two types of knowledge, actual knowledge and constructive knowledge.

[15] The Provisions of the Supreme People's Court on Several Issues Concerning Application of Law in the Trial of Cases Involving Disputes about Infringing Right to Internet Dissemination of Information (2013), Art. 8 (hereinafter "Provisions").

[16] 17 U.S.C. §512(c)(1)(A).

[17] Directive 2000/31/EC, Art. 14(1).

[18] Telemedia Act, Art. 10.

[19] Regulation on the Protection of the Right to Internet Dissemination of Information, Art. 22(3) (hereinafter "Provisions").

### 3.1 "Red Flag" Standard in the US

"That actual knowledge standard is high, and by itself does not reach an entity that willfully ignores blatant indications of infringement,"[20] which means actual knowledge is difficult to prove. Therefore, the parties involved always dispute what constitutes constructive knowledge of an infringing activity. According to the House Report (Commerce Committee), the provisions concerning constructive knowledge in the DMCA can best be described as a "red flag" test, which means if the service provider becomes aware of a "red flag" from which infringing activity is apparent, it will lose the limitation of liability if it takes no action.

The "red flag" test has both a subjective and an objective element. In determining whether the service provider was aware of a "red flag", the subjective awareness of the service provider of the facts or circumstances in question must be determined. However, in deciding whether those facts or circumstances constitute a "red flag", in other words, whether infringing activity would have been apparent to a reasonable person operating under the same or similar circumstances, an objective standard should be used.[21]

In the view of David Nimmer, the knowledge requirement required by the "red flag" test is more favorable to ISPs than the previous contributory infringement, which is not "what a reasonable person would have deduced given all the circumstances, but rather whether the service provider deliberately proceeded in the face of blatant factors of which it was aware,"[22] so as to "avoid rewarding those (ISPs) who adopt the posture of an ostrich."[23] In other words, the infringing flag must be "brightly red indeed – and be waving blatantly in the provider's face – to serve the statutory goal of making 'infringing activity… apparent.'"[24] Nimmer's interpretation of the "red flag" test has been widely quoted by US courts.[25] As for what constitutes a"red flag", the legislative history suggests a high standard:

> The infringing nature of such sites shall be apparent from even a brief and casual viewing, e.g., sites typically use words such as "pirate", "bootleg", or slang terms in their URL and header information to make their illegal purpose obvious … to Internet users; but just one or more well known photographs of a celebrity at a site cannot be treated as red flag.[26]

By following this high standard, US courts have held that the following circumstances did not qualify as a "red flag": (1) if investigation of the "facts and circumstances" is required to identify material as infringing, then those facts and

[20] Nimmer (2003).

[21] H.R. REP. 105551(II), 53.

[22] *See* D. Nimmer, *supra* note 20, at 358.

[23] *Id*.

[24] *Id*.

[25] *See Io Group, Inc. v. Veoh Internets, Inc*., 586 F.Supp.2d 1132, 1148 (N.D. Cal. 2008); *Corbis Corporation v. Amazon.com*, 351 F.Supp.2d 1090, 1108 (W.D. Washington 2004).

[26] *See* H.R. REP. 105-551(II), *supra* note 21, at 57–58.

circumstances are not "red flags";[27] (2) hosting of password-hacking websites is not a per se "red flag" of infringement;[28] (3) the disclaimer stating that "copyrights of these files remain the creator's. I do not claim any rights to these files, other than the right to post them" was not a "red flag" of infringement;[29] (4) describing photographs as "illegal" or "stolen" is not a "red flag";[30] and (5) the professionally created nature of uploaded content does not constitute per se "red flag" of infringement.[31] However, a notification of specific infringement from a third party, such as an Internet user, rather than from a copyright owner, might meet the "red flag" test.[32] The case law in the US examining facts, such as hosting of password-hacking websites, statement of rights disclaimers, describing content as "illegal" or "stolen", which always indicate the illegal nature of content, and finding that these circumstances do not establish a red flag suggests that establishing a red flag is a very high burden for any copyright owner alleging infringement.

Even though US courts recognize the existence of "red flags", an ISP will not definitely possess "red flag" knowledge, because another subjective requirement still needs to be met, namely the ISP must subjectively know of the existence of a "red flag", which is also difficult to prove. As Judge Howard stated in *Io v. Veoh*, "although one of the works did contain the plaintiff's trademark several minutes into the clip (which might qualify for red flag), there is no evidence from which it can be inferred that Veoh was aware of, but chose to ignore, it."[33] Therefore, constructive knowledge of a hosting ISP is not easy to establish through applying the "red flag" test.

[27] *UMG Recordings, Inc. v. Veoh Internets, Inc*., 665 F.Supp.2d 1099, 1108 (C.D.Cal. 2009).

[28] *Perfect 10, Inc. v. CCBill, LLC*, 488 F.3d 1102, 1114 (9th Cir. 2007). As stated by the court, the burden of determining whether passwords on a website enabled infringement is not on the service provider. The website could be a hoax, or out of date. The owner of the protected content may have supplied the passwords as a short-term promotion, or as an attempt to collect information from unsuspecting users. The passwords might be provided to help users maintain anonymity without infringing on copyright. There is simply no way for a service provider to conclude that the passwords enabled infringement without trying the passwords, and verifying that they enabled illegal access to copyrighted material. We impose no such investigative duties on service providers.

[29] *Id*. As stated by the court, contrary to Perfect 10's assertion, this disclaimer is not a "red flag" of infringement. The disclaimer specifically states that the webmaster has the right to post the files.

[30] *Id*. As stated by the court, describing photographs as "illegal" or "stolen" may be an attempt to increase their salacious appeal, rather than an admission that the photographs are actually illegal or stolen, and shouldn't place the burden of determining whether photographs are actually illegal on a service provider.

[31] *Io Group, Inc. v. Veoh Internets, Inc*., 586 F.Supp.2d 1132, 1149 (N.D. Cal. 2008). As stated by the court, with the video equipment available to the general public today, there may be little, if any, distinction between "professional" and amateur productions.

[32] *UMG Recordings, Inc. v. Shelter Capital Partners, LLC*, 667 F.3d 1022, 1040 (9th Cir. 2011). In this case, the Court made a very interesting differentiation between the notifications from copyright owner and the third party. The CEO of Disney sent an e-mail to a Veoh investor, which stated that the movie *Cinderella III* and various episodes were available on Veoh without Disney's authorization. The court decided that this e-mail did not qualify as a red flag for the following reason: as a copyright holder, Disney was subject to the notification requirements in §512(c)(3), which this informal e-mail failed to meet. However, if this notification had come from a third party, such as an Internet user, it might meet the "red flag" test, since it specified particular infringing material.

[33] *See Io Group, Inc. v. Veoh Internets, Inc*., *supra* note 31, at 1149.

Besides the "red flag" test provided in DMCA §512, according to common law, willful blindness is tantamount to knowledge.[34] Therefore, willful blindness can also lead to an ISP's liable for the primary infringement committed by its users. By referring to case law, one can find that a person is "willfully blind" if the person is "aware of a high probability of the fact in dispute and consciously avoided confirming that fact."[35] From this definition, it appears that the liability resulting from "willful blindness" can be based on a defendant's general knowledge of infringement (awareness of a high probability of the fact in dispute). However, as mentioned before, the "no monitoring responsibility" clause in DMCA §512 prohibits a court from concluding secondary liability based on an ISP's general knowledge of infringement.[36] Therefore, when applied to a hosting ISP's liability, the doctrine of "willful blindness" should be strictly interpreted. As for how strict the interpretation should be, in a recent case the US District Court for the Southern District of New York held that what disqualifies the service provider from DMCA §512 protection is blindness to "specific and identifiable instance of infringement."[37] The court's interpretation turns the "willful blindness" test back to an analysis of the "red flag" test because the red flag should be a specific and identifiable instance of copyright infringement. If so, then the "willful blindness" doctrine seems no more than to reaffirm the "red flag" test. However, in the long term, more relevant case law is needed to determine how precisely "willful blindness" shall be applied.

### 3.2 Hosting ISPs' Knowledge in Germany

In Germany, "actual knowledge" is called "positive knowledge" (*positive Kenntnis*).[38] According to the dominant legal opinion, positive knowledge of concrete and specified information is understood in terms of direct intent (*dolus directus*),[39] which means "should know" in the sense that gross negligence is not enough to constitute positive knowledge.[40] Therefore, it is common for German courts to conclude that negligent ignorance is not equal to the positive knowledge required by law.[41] However, a hosting ISP cannot be completely immunized from monetary claims if it does not know of the infringements by reason of its gross

[34] *Tiffany (NJ) Inc. v. eBay, Inc*., 600 F.3d 93, 110 (2d Cir. 2010).

[35] *United States v. Aina-Marshall*, 336 F.3d 167, 170 (2d Cir. 2003) (quoting *United States v. Rodriguez*, 983 F.2d 455, 458 (2d Cir. 1993)).

[36] *See Viacom Intern., Inc. v. YouTube, Inc*., *supra* note 5, at 35. As stated by Federal Court of Second Circuit, §512(m) is explicit: DMCA safe harbor protection cannot be conditioned on affirmative monitoring by a service provider. For that reason, §512(m) is incompatible with a broad common law duty to monitor or otherwise seek out infringing activity based on general awareness that an infringement may be occurring.

[37] *Viacom Int'l Inc. et al. v. YouTube et al.*, 07 civ. 2103 (LLS), 32 (S.D.N.Y. 18 April 2013).

[38] Fitzner (2011).

[39] *Id.*

[40] Munich Court of Appeal, *Gewerbeschädigende Äußerungen in einem Meinungsforum im Internet*, 2002 MMR 612.

[41] Spindler et al. (2008).

negligence, because under Art. 10 of the German Telemedia Act, in order to enjoy the immunity, a hosting ISP must not know any fact or circumstance from which the illegality of the conduct or information is apparent.[42] Nevertheless, the gross negligence provided in Telemedia Act Sec. 10 limits its application only to deliberately gross negligence, and can only be found in clear and obvious cases,[43] such as where the concrete evidence of committing definitely illegal conduct or absolutely illegal content displays in front of the hosting ISP.[44]

Telemedia Act Sec. 10 includes the language "*keine Kenntnis von der rechtswidrigen Handlung oder der information*", which was inherited from Sec. 5 of the 1997 Teleservices Act (Teledienstgesetz) and can be translated in English as "no knowledge of the illegal conduct or information". However, in the German language context, it can be interpreted in two ways, one of which is "no knowledge of the illegal conduct and no knowledge of illegal information" and the other being "no knowledge of the illegal conduct and no knowledge of information." There has been considerable disagreement as to how Teleservices Act Sec. 5 should be interpreted. According to the German legislators, the term "illegal" in Art. 14 of the Directive on electronic commerce only points to conduct but is irrelevant to interpreting the term "information," so for the "information," the knowledge requirement can be fulfilled if the hosting ISP knows the existence of the information regardless of whether it also knows the illegality of this information or not.[45] However, Gerald Spindler believes that the German legislators unintentionally misunderstood Art. 14 of the Directive when transplanting it into German law; on the contrary, the Directive on electronic commerce does not differentiate between conduct and information with regard to illegality.[46] The circumstances are, however, different. For example, in the case of illegal conduct, the information itself is legal, and only the conduct such as the unauthorized copying or publishing of this information is illegal. In the case of illegal information, the information itself is illegal, such as pornography, violent or Nazi content.[47] After the *Google AdWords* case concluded by the European Court of Justice (ECJ), the debate on this question seemed to end, because the ECJ had specifically declared that a service provider cannot be held liable for data which it has stored at the request of an advertiser, unless, it had knowledge of the unlawful nature of the data or of the advertiser's activities, but failed to act expeditiously to remove or to disable access to the data concerned.[48] A month later, the German Federal Supreme Court followed the ECJ's opinion in the case *Google AdWords*,[49] and since then in Germany a hosting ISP

[42] Telemedia Act Sec. 10(1).

[43] *See* J. Fitzner, *supra* note 38, at 287.

[44] Düsseldorf District Court, *Markenrechtsverletzung durch Onlineauktion*, 2003 MMR 120–127.

[45] BT-Drs. 14/6098, S. 25, (quoting G. Spindler, et al., *supra* note 41, at 1531).

[46] *See* Spindler, *supra* note 41, at 1531.

[47] *Id.*

[48] Case C-236/08 to C-238/08, *Google France, Google, Inc. v Louis Vuitton Malletier, Viaticum SA, Luteciel SARL, Centre national de recherche en relations humaines (CNRRH) SARL, Pierre-Alexis Thonet, Bruno Raboin, Tiger SARL*, Para. 120.

[49] German Federal Supreme Court, 29 April 2010, Case No. I ZR 69/08 – *Vorschaubilder*.

must have knowledge of the illegality of information in order to trigger its responsibility to delete or block such information.

With development of filtering technologies, many hosting ISPs have installed filtering programs in order to reduce copyright infringement. Before any content can be uploaded it is scanned by the filtering program, so technically this content is known by the filtering program. This raises the question of whether the information that is "known to" a filtering program is legally equated to the knowledge possessed by the hosting ISP. The "knowledge" of the filtering program if attributed to the ISP may remove the hosting ISP from its "safe harbor". It is generally accepted that, because a hosting ISP not only needs to know the information but also the illegality of the information, and the machine cannot displace a human in checking whether the information is infringing or not, then the knowledge of the filtering program should not be seen as fulfilling "knowledge" in the sense of Telemedia Act Sec. 10.[50]

Generally speaking, it is not easy to prove that a hosting ISP has knowledge of copyright infringement as understood in Telemedia Act Sec. 10. As noted by Thomas Hoeren, if there is no notification of an alleged infringement, then it is legally presumed that the provider has no sufficient knowledge of any infringing action and, consequently, the ISP is not responsible.[51]

### 3.3 "Should Know" in China

In China, a hosting ISP's actual knowledge of infringement can rarely be proved, except where the ISP receives official notice from the copyright owner by post, fax or e-mail to complain about the infringement.[52] As for what constitutes "should know", namely "justifiable reason to know" as provided in the Regulation, some Chinese courts have concluded the existence of "red flags" as being equivalent to "should know". In the case *Hua Xia Shu Ren v. Youku.com*, the Handian District Court concluded that the defendant, Youku.com, should have known of the infringements involved based on the following facts: (1) a large number of infringing videos, most of which were marked "copyright is reserved by Hua Xia Shu Ren", were claimed to be offered by an Internet user, the so-called "*Qilingjiao*"; and (2) the defendant also propagated its service as "Youku being a good learning club".[53] In this case, the videos marked "copyright is reserved by Hua Xia Shu Ren" can be treated as a qualified "red flag" in the context of the US "red flag" test, because the claim of "copyright reservation" has already made the infringing nature of relevant videos obvious, just like the clip containing the plaintiff's trademark for several minutes in the case *Io v. Veoh*.[54] However, rather

[50] *See* Spindler, *supra* note 41, at 1531–1532. Also *see* J. Fitzner, *supra* note 38, at 289–290.

[51] Hoeren and Yankova (2012).

[52] *See* Provisions, *supra* note 15, Art. 13.

[53] *Hua Xia Shu Ren v. Youku.com*, No. 9200 Hai Min Chu Zi (2008).

[54] *See Io Group, Inc. v. Veoh Internets, Inc*., *supra* note 31, at 1149. In the decision, the court did not directly conclude that the clip qualified for "red flag", but it can be implied from the phrasing: "Although one of the works did contain plaintiff's trademark several minutes into the clip, there is no evidence from which it can be inferred that Veoh was aware of, but chose to ignore, it."

than applying both prongs of the US "red flag" test, the Handian District Court decided the question of liability without considering whether the defendant knew of the "red flag". Thus, the Handian District Court made hosting ISPs more easily subject to secondary liability than they would be under the two pronged "red flag" test in the US.

Thereafter, scholars in China increasingly proposed the US "red flag" test. In particular, Prof. QianWang, systematically began advocating for the implementation of the US "safe harbor" provision in China, and wrote several influential articles about the US "red flag" test.[55] Eventually, Chinese courts determined that the application of the "red flag" test consists of two steps, one of which is the existence of "red flag", and the other is that a hosting ISP also knows of the "red flag". According to the new Provision issued by the People's Supreme Court, the some factual circumstances under which a hosting ISP would be found to meet the "should know" standard are: (1) hot-play audio–video located on the homepage, other main pages, or other places of a website which can be easily identified by an ISP; (2) taking the initiative to choose, edit, sort or recommend the hot-play audio–video works, or setting a special top list for them; and (3) other circumstances under which the relevant works, performances, audio recordings and sound or video recordings can be easily determined that they are offered without authorization, but the ISP then fails to take reasonable measures to prevent the copyright infringement.[56]

After examining the specific circumstances enumerated above in the Provision, the shadow of the US "red flag" test can clearly be seen. The first circumstance demonstrates a concrete example fulfilling the "red flag" test. To be more precise, in terms of hot-play[57] audio–video works available on the Internet for free, hosting ISPs should know that these works are infringing copies without need of further investigation, since the copyright owners would not make their popular audio–video works available on the Internet without charge when these works are still considered hot-play. Therefore, these infringements are sufficient to qualify them as "red" flags. Furthermore, during its daily operations, the ISP certainly checks its own homepage and other main pages, so if these infringed hot-play audio–videos are being shown on these sites, the hosting ISP cannot deny it knows that these are flashing "red flags". For the second point, the facts depicted by it look more like direct infringements rather than indirect infringement subject to the "red flag" test, because if the hosting ISP takes the initiative to choose, edit, sort or recommend the hot-play audio–video works, it is actively involved in the infringement and should be defined as a direct infringer rather than secondary or contributory infringer. Nevertheless, if it actively participates in the copyright infringement, itclearly should know the infringement is taking place. The third

[55] Wang (2008).

[56] *See* Provisions, *supra* note 15, Art. 12.

[57] "Hot-play" is a term that can always be found in the decisions made by Chinese courts, and finally was incorporated into the Provisions by People's Supreme Court. In terms of relevant decisions, "hot-play" has always been used to describe the audio–video works which are newly distributed, popular and still on screen.

circumstance can be seen as a substantial copy of the "red flag" test but expressed from another perspective.

Besides setting specific "should know" circumstances for hosting ISPs, concerning all types of ISPs, the Provision also lists some others factors that need to be comprehensively assessed when concluding "should know". These are: (1) the characters of service offered by ISPs, the ways of offering service, the possibility of leading to infringements through its service, and ISPs' capability of managing information; (2) the types and fame of transmitted works, performances, sound recordings and video recordings, and whether or not the infringement is obvious; (3) whether the ISPs take the initiative to choose, edit, modify and recommend the works, performances, audio recordings and audio–video recordings; (4)whether the ISPs adopt reasonable measures to prevent infringements actively; (5) whether the ISPs set convenient processes to receive the infringing notices, and whether the ISPs respond to them reasonably; (6) whether the ISPs take reasonable responding measures against repeat infringements committed by the same Internet user; and (7) the other elements which need to be considered.[58]

By analyzing the factors enumerated above, one can find that, compared to the "red flag" test, they seem more likely to regulate the commercial model of ISPs rather than focusing on whether the ISPs know of the existence of concrete infringement. Except for the second and third factors, which are directly relevant to the knowledge of ISPs, the other factors require the ISPs to fulfill a certain duty of care so as to reduce infringement. In addition, the People's Supreme Court also enumerates a particular instance, under which the People's courts can legally presume that ISPs have knowledge that their Internet users are infringing a copyright owner's right to network dissemination of information, as follows: where the ISPs recommend the hot-play audio–video works by means of setting lists, content indexes, describing paragraphs, content introductions, etc., when offering Internet service, and the public can access these works through directly downloading, browsing or other ways.[59] Based on the similar reasons referred to above, this particular instance is more like a direct copyright infringement rather than an indirect infringement, because if an ISP recommends any audio–video works, these audio-video works can be seen as being its own offering from a legal perspective, and thus it should be subject to direct liability, if there is any copyright infringement.

Based on the above discussion of imputed knowledge compared with judicial practice in the US, Chinese courts seem to interpret imputed knowledge more broadly and extending it to cover not only the "red flag" test, but also to cover direct infringement in an effort to compel the hosting ISPs to undertake certain duties so as to regulate their business model. In contrast to what happens in China, in Germany it seems that the imputed knowledge can only be found by the courts in quite limited circumstances.

[58] *See* Provisions, *supra* note 15, Art. 9.

[59] *Id*, Art. 10.

## 4 Repeating Infringements

Since hosting ISPs need not to undertake general monitoring responsibility for checking the content uploaded by their users, copyright owners rely heavily on certain ex post facto measures to protect their rights, such as measures against repeating infringements. In each country there are different measures required against repeating infringements. In the US, the "safe harbor" provision requires hosting ISPs to take necessary measures against repeat infringers. In Germany, *Störerhaftung* (disturber's liability) requires hosting ISPs to take reasonable measures to prevent the same infringing content from being uploaded again. In China, the Provision issued by the People's Supreme Court seems to adopt a mixed solution, which means hosting ISPs are required to take necessary measures against both repeat infringers and repeated infringement of the same copyrighted content.

### 4.1 Repeat Infringer Policy in the US

In the US, in order to enjoy liability limitation, an ISP must "have adopted and reasonably implemented, and informed subscribers and account holders of the service provider's system or Internet of, a policy that provides for the termination in appropriate circumstances of subscribers and account holders of the service provider's system or Internet who are repeat infringers."[60] After examining this provision, focus is on infringing users rather than on infringing content, which can be properly called a repeat infringer policy, and ISPs' clients must also be informed of this policy.

The repeat infringer policy is closely related to the DMCA "notice-take down" mechanism. First, only after a qualified notification has been sent, which is sufficient for the hosting ISP to locate the infringing content, will the court investigate whether the hosting ISP has properly implemented a policy against repeat infringing. For example, in the case *Perfect 10, Inc. v. CCBill, LLC*, the notice sent by Perfect 10 only identified the website that contained the alleged infringing materials, but did not identify the URLs of the images or identify which of its images were being infringed, so the notice failed to provide IBill with enough information to locate the infringing materials.[61] Therefore, the court found that this notice could not support the claim that IBill had failed to reasonably implement its repeat infringer policy.[62] Second, a hosting ISP must name a proper agent to receive notifications of complaint. In *Ellison v. Robertson*, the defendant had changed the e-mail address to which "the infringement notifications were suppose to have been sent", and "failed to provide for forwarding of message sent to the old address or notification that the e-mail address was inactive", so the court found that the defendant did not have an effective notification agent in place at the time when the

[60] 17 U.S.C. §512(i)(1)(A).

[61] *See Perfect 10, Inc. v. CCBill, LLC*, 340 F Supp 2d 1077, 1090 (C.D. Cal, 2004). This opinion has been upheld by 9th Circuit Court in the appealing instance; *see Perfect 10, Inc. v. CCBill, LLC*, *supra* note 28, at 1113.

[62] *Id*.

alleged infringing activities occurred, and thus had not reasonably implemented its policy against repeat infringers.[63] Third, unlike the "notice-take down" mechanism, notices of copyright infringement from a non-party are relevant in deciding whether the repeat infringer policy is properly implemented. In the case of *Perfect 10, Inc. v. CCBill, LLC*, the appeals court held that DMCA §512(i)(1)(A) required it to assess the service provider's "policy" rather than how the service provider actually treated a particular copyright owner, so defendants' actions towards non-parties were relevant in determining whether defendants had reasonably implemented their repeat infringer policy.[64]

Since there is public policy against repeat infringers, it is important to define and discuss what "repeat" ought to mean in the context of infringement. However, it seems that US courts did not exert much effort in interpreting the concept of repeat infringer. In the case *Perfect 10, Inc. v. CCBill, LLC*, the court found that both of the following circumstances conform to the repeat infringer policy: (1) upon receiving notice from the plaintiff that complied with the DMCA's notification requirements, defendant–IBill had suspended the offending website's account[65]; and (2) the defendant Internet Key would ban a webmaster from its age-verification service after it had received three notifications regarding the website of any particular webmaster.[66] Therefore, at least in the US District Court for the Central District of California, it is tolerable if an ISP does not enforce its repeat infringer policy against an Internet user after its second infringement. Additionally, it is worth noting that Congress requires reasonable implementation rather than perfect implementation.[67] Hence, although an ISP's policy can be easily sidestepped by infringing Internet users, such as opening a new account after their original accounts have been terminated, the efforts to sidestep the defendant's policy do not amount to a failure of implementation on the part of the defendant.[68] Moreover, to identify and terminate repeat infringers, the ISPs also do not need to track users in a particular way to affirmatively police users for evidence of repeat infringement.[69] However, impeding the proper implementation of this policy is prohibited. In the case of *Aimster*, an encryption system was built into the defendant's system which prevented it from knowing which users were transmitting which particular file, so actually the repeat infringer policy could never be implemented, and based on this the court concluded that the defendant failed to satisfy the threshold requirement of DMCA 512(i)(A).[70]

[63] *See Ellison v. Robertson*, 357 F3d 1072, p. 1080 (9th Cir, 2004).

[64] *See Perfect 10, Inc. v. CCBill, LLC*, *supra* note 28, at 1113.

[65] *See Perfect 10, Inc. v. CCBill, LLC*, *supra* note 61, at 1090.

[66] *Id*, at 1093.

[67] *Id*, at 1089.

[68] *Corbis Corp. v. Amazon.com, Inc*., 351 F.Supp.2d 1090, 1103 (W.D. Wash. 2004). *See also Io Group, Inc. v. Veoh Internets, Inc*., *supra* note 31, at 1143–1145.

[69] *Id*, *Io Group, Inc. v. Veoh Internets, Inc*.

[70] *Aimster*, 334 F.3d 643, 655 (7th Cir. 2003).

### 4.2 *Störerhaftung* – Disturber's Liability in Germany

As discussed in the section on "Hosting ISPs' Knowledge in Germany", a hosting ISP's knowledge of infringement is difficult to prove without proper notification from the copyright owners, so liability based on knowledge can rarely be found by a court. However, German law offers an alternative basis on which to impose hosting ISPs' liability, *Störerhaftung*, which can be translated as "disturber's liability" in English. According to Art. 97 of the German Copyright Act.,

> Any person who infringes copyright or any other right protected under this Act may be required by the injured party to eliminate the infringement or, where there is a risk of repeated infringement, may be required by the injured party to cease and desist. Entitlement to prohibit the infringer from future infringement shall also exist where the risk of infringement exists for the first time.[71]

"Disturber's liability" is a kind of liability that requires the responsible party to prevent certain infringements from occurring again in the future. Because the Telemedia Act Sec. 10 only limits the monetary damages liability of qualified hosting ISPs, the other remedies such as "disturber's liability" can remain unaffected by Sec. 10 of the Act. Currently, whether the hosting ISPs should face "disturber's liability" has become a main point of contention by parties before German courts. Matthias Leistner notes that if a site runs an automatic processing system (such as a platform automatically processing the contents uploaded by its users), it is unpractical for it to acquire the knowledge or control over the information transmitted in the system. However, in order to ensure it is free of liability in this way, it must adapt itself in the future to qualify for the following requirement, namely, based on the intensified duties established in the context of "disturber's liability", it should at least take minimal control over the transmitted information after receiving clear notices regarding concrete infringements.[72]

The German Federal Supreme Court made a fundamental and proper development of the breadth of "disturber's liability" for hosting ISPs. Upon receiving evidence regarding a concrete and obvious infringement, the relevant ISP must not only block this concrete infringement, but it is also responsible for taking all possible and reasonable measures to prevent substantially similar infringements from occurring in the future.[73] As for what constitutes possible and reasonable measures, German courts have differing opinions. In *Sharehoster II*, the Hamburg Court of Appeal followed a strict approach to an ISP's monitoring duty, and required the defendant, after being notified by the plaintiff of a particular infringement, to undertake a preventive search (both automatic and manual) of all hosted content in order to identify the material infringing the plaintiff's rights, and to check all the files that were uploaded by users who previously uploaded infringing content.[74] The Düsseldorf Court of Appeal, by contrast, seems to have

[71] Copyright Act, Sec. 97(1).

[72] Leistner (2012).

[73] *Id*, at 724.

[74] *Sharehoster II*, 2010 *MMR* 51, 53 (quoting Matulionyte and Nérisson 2011).

favored the hosting provider, and found that the measures applied by the ISP (essentially the same as those in the case before the Hamburg court) were sufficient, but the monitoring duties required by the plaintiff, such as word filtering of titles, manual searching and blocking IP addresses were unreasonable.[75]

Moreover, academics in Germany are also enthusiastic about setting a proper criterion for "disturber's liability". In Leistner's opinion, because of E-Commerce Directive Art. 15 (Sec 7(2) Telemedia Act), no general active monitoring responsibility should be taken into account. In any case, if legal business models are worthy of protection, they are usually only obliged to take economically reasonable filtering conducts (usually only automatic measures are feasible).[76] However, when analyzing the ISP's legal business model it is still necessary to distinguish between dangerous and neutral business models. The former means a business model that could easily result in infringements based on its previous advertising, design, and the funding structure of its platform, while the latter means a business model that is not particularly friendly to infringements due to its marketing, structure of platform and benefiting model.[77] For the active disturber (the one who runs the illicit model), if it still operates a legal business model, then exerting further control and duties are reasonable so as to make the particular illicitly structured business model neutral again.[78] From the above statement, the hosting ISP's intent, which can be deduced from its business model, is an important factor when deciding how broad the "disturber's liability" should be. This means if a hosting ISP has the intent to promote the infringing use of its platform, it is reasonable to ask it to take more responsibility in the context of "disturber's liability".

In the case of *Rapidshare*, the German Federal Supreme Court also delivered a similar opinion. It concluded that when deciding the scope of responsibilities as a disturber, the following two factors must be considered: (1) whether or not the business model of a hosting ISP is designed for infringements from the beginning; and (2) whether it promotes the infringing use of its service by its own measures.[79] If a hosting ISP induces copyright infringements committed on a substantial scale, it is reasonable for it to take comprehensive and regular control over the "links collections"[80] that refer to its service.[81]

To conclude, unlike the repeat infringer policy in the US, in Germany substantial measures are required to be taken against repeat infringement of the same content rather than repeat infringers. However, similarly to the US, these measures taken by hosting ISPs should be possible and reasonable, but they do not

[75] *Rapidshare*, 2010 *MMR* 483, 484 (quoting R. Matulionyte and S. Nérisson, at 66–67).

[76] M. Leistner, *supra* note 72, at 725.

[77] *Id.*

[78] *Id.*

[79] German Federal Supreme Court, 15 August 2013, case No. I ZR 80/12 – *Rapidshare*, para. (b).

[80] "Link collections" means the collections of search results after searching for specific content through search tools. For instance, if a person searches keywords of "alone in dark, Rapidshare" in Google, the results are links from which a person can download "alone in dark" residing on Rapidshare.

[81] German Federal Supreme Court, *supra* note 79, para. (c).

need to be perfect. As for what the possible and reasonable measures are, that depends on the hosting ISPs' intent as mirrored in their business model. This means that the more likely a hosting ISP's business model is to result in infringements, then more sophisticated measures against repeat infringement of content are possible and reasonable. In addition, the enforcement of disturber's liability in Germany is also relevant to the "notice-take down" mechanism, because generally a proper notification from the copyright owner needs to be sent so as to trigger disturber's liability.

### 4.3 Repeat Infringement from the Same Internet User in China

Although the Regulation adopts the "notice-take down" mechanism, it does not include a provision requiring ISPs to take action against repeat infringers or the repeat infringement of the same content. However, the General Principles of the Civil Law of the People's Republic of China, as a fundamental legal document protecting private rights, provides a general liability rule which is quite similar to the "disturber's liability" in German civil law as follows: (1) cessation of infringements, (2) removal of obstacles, and (3) elimination of dangers.[82] Based on the rational embodied in the Chinese "disturber's liability", some courts require hosting ISPs to take essential measures against repeat infringements. For instance, in the case *Yinian v. Taobao*, although the defendant Taobao had already deleted the infringing content after receiving complaints which all pointed to one account (the owner of this account was another defendant in this case), this account still existed even after seven complaints. Based on this fact, the Court then concluded that the defendant had not fulfilled its duty of care, thus it faced contributory liability.[83] In the case *Han Han v. Baidu*,[84] the plaintiff sent notification complaining that one of his books *Xiang* had been uploaded onto the defendant's literature-sharing platform without permission.[85] After receiving notice, the defendant deleted the infringing content; however, the same infringing content under a different title could still be accessed on the defendant's platform.[86] Based on these facts, the Court concluded that the defendant had not taken sufficient measures to prevent the infringing

[82] General Principles of the Civil Law of the People's Republic of China, Art. 134. The legislators in China used Art. 1004 of German Civil Law as an important reference, which provides that "If the ownership is interfered with by means other than removal or retention of possession, the owner may require the disturber to remove the interference. If further interferences are to be feared, the owner may seek a prohibitory injunction", when drafting Art. 134. This kind of "*Störerhaftung*" has also been reaffirmed by the newly adopted China Tort Law in Art. 15.

[83] *Yinian v. Taobao*, No. 40 Hu Yi Zhong Min Wu (Zhi) ZhongZi (2011). This case was published in the Bulletin of People's Supreme Court (Vol. 1, 2012) as a guiding case.

[84] Han Han is one of most distinguished young writers who has many fans in China, and in May 2010, he was named one of most influential people in the world by Time magazine. The other party, Baidu, can be seen as the Chinese Google, and is one of the most successful Internet companies in China. Therefore, the dispute between these two parties attracted considerable attention and, finally, this case was selected as one of ten annual IP cases (2012) by the People's Supreme Court.

[85] *Han Han v. Baidu*, No. 5558 Hai Min Chu Zi (2012).

[86] *Id*.

content from being transmitted through its platform, despite the fact that the defendant claimed it had run an anti-piracy system.[87]

By comparing the two cases cited above, it appears that that according to the first case, courts that require the hosting ISPs to terminate accounts repeatedly used for infringing activities are likely to adopt the US approach. By contrast, by deducing from the second case, courts requiring the hosting ISPs to prevent the same infringing content from being accessed again are more likely to follow the German approach. This difference shown in these two cases demonstrates that Chinese courts know of the necessity of requiring hosting ISPs to prevent repeat infringements, but they are not entirely sure which approach to adopt. This struggle is also reflected in the newly issued Provision. The draft of the Provision states that the ISP should take reasonable measures to prevent the infringement of the same content from occurring again, which is typical of the German approach.[88] However, the final version of Provision includes a more nuanced expression – whether the ISPs take reasonable measures against repeat infringements made by the same Internet user.[89] This can be understood in two ways: first, if "repeat" is interpreted as "same", namely, the same infringements made by the same Internet user, it is a "double requirement of identity" standard such as that advocated by the EU Advocate General in the case *L'Oréal SA v. eBay*;[90] second, if "repeat infringement" is understood more broadly, meaning if all infringements after the first one made by the same Internet user count as repeat infringements, then it looks more like a rule against repeat infringers, because terminating the repeat infringer's account seems the only efficient way of getting rid of these repeat infringements. As for what constitutes reasonable measures, in the case *Han Han v. Baidu*, the court held that manual monitoring measures must not be imposed, because they are too burdensome to be continuous. Regarding technical measures, whether they are reasonable depends on the current technical level and will change with the development of new technologies.[91] Furthermore, the court held that the measures need not be perfect and that the following measure is inappropriate, namely, using the author's name plus the title of the work as keywords to filter out infringing content, because that in turn might block considerable legal content.[92]

[87] *Id.*

[88] The Provisions of the Supreme People's Court on Several Issues Concerning Application of Law in the Trial of Cases involving disputes about Infringing Right to Internet dissemination of information (draft published for discussion), Art. 8 (6).

[89] *See* Provisions, *supra* note 15, Art.9(6).

[90] *L'Oréal SA v. eBay*, C–324/09 (AG's Opinion), para. 182. In this case, the AG first admitted that nothing in Directive 2004/48 would prohibit injunctions against the intermediary requiring not only the prevention of the continuation of a specific act of infringement but also the prevention of repetition of the same or a similar infringement in the future if such injunctions are available under national law. However, he also emphasized legal certainty and that an injunction should not impose impossible, disproportionate or illegal duties such as a general obligation to monitor. He concluded that an appropriate limit for the scope of injunctions may be that of a double requirement of identity.

[91] *See Han Han v. Baidu*, *supra* note 85.

[92] *Id.*

By comparing the rules against repeat infringement in the US, Germany and China, it appears that the US rules focus on punishing repeat infringers, the German rules focus more on preventing the repeat infringement of content, and the rules in China can be understood as a mixed solution, which not only asks hosting ISPs to prevent the repeated infringing of content based on the "double requirement of identity" (a limited German approach), but also requires hosting ISPs to terminate the accounts of repeat infringers (a US approach). Of these three approaches, the German one offers the best copyright protection, because the US approach can easily be sidestepped by creating another account, while the Chinese approach imposes the restriction of "double requirement of identity" over repeat infringement of content. However, from the aspect of practice, some hosting ISPs in the US and China have already taken technical measures to block the same infringing content from being uploaded again. For instance, Veoh, a video-sharing website in the US, has adopted means for generating a "hash", or digital "fingerprint", for each video, which essentially enables Veoh to terminate access to any other identical files and prevent additional identical files from ever being uploaded by any user.[93] In China, Tudou, a video-sharing website, has established a database called "collection of black content", and any video which has been disputed will be marked with a fingerprint and put into the database for comparison with videos uploaded thereafter, so as to filter out repeat infringing content.[94] Therefore, despite the different rules, the hosting ISPs in these three countries tend to adopt similar measures against repeat infringement. Furthermore, in all three jurisdictions a common restriction has been set on required measures, which is "reasonable" rather than "perfect".

## 5 Benefit from Infringements

In US common law, directly benefiting from infringements is one of two prongs for concluding vicarious liability, and the other is having the right and ability to control the infringements.[95] The US "safe harbor" provision also adopts a similar rule to regulate hosting ISPs' secondary liability.[96] By contrast, in Germany and China, benefiting or profiting from infringements is not an independent culpable element when concluding liability. However, when hearing cases involving hosting ISPs' secondary liability, courts in Germany and China always take hosting ISPs' benefit or intent to benefit into account.

[93] *See Io Group, Inc. v. Veoh Internets, Inc*., *supra* note 31, at 1143.

[94] During a workshop about "video-sharing website's secondary liability" held in Center for Studies of Intellectual Property Rights of Zhongnan University of Economics and Law, the former legal director, Mr. Guangliang Cai delivered an introduction about the anti-piracy measures adopted by Tudou, which covered the database of black content. The relevant statement can also be found in Tudou's copyright policy from its website, *see* http://www.tudou.com/about/cn/copyright.html.

[95] *See Gershwin Publ'g Corp. v. Columbia Artists Mgmt., Inc.,* 443 F.2d 1159, 1162 (2d Cir. 1971).

[96] *See* 17 U.S.C. §512 (c)(1)(B). According to this Article, if a hosting ISP wants to be exempted from secondary liability, it should not receive a financial benefit directly attributable to the infringing activity, in a case in which the service provider has the right and ability to control such activity.

### 5.1 Direct Benefit in the US

According to DMCA §512(c)(1)(B), in the US, if a hosting ISP wants to be exempted from secondary liability, "it should not receive a financial benefit directly attributable to the infringing activity, in a case in which the service provider has the right and ability to control such activity". In a literal sense, the substantial contents of this provision are quite similar to the vicarious liability rule in US common law. However, the Congressional report specifically states the liability limitation provided in DMCA 512 "protects qualifying service providers from liability for all monetary relief for direct, vicarious and contributory infringement."[97] Therefore, it seems that the "financial benefit" and "right and ability to control" in DMCA 512(c)(1)(B) may be interpreted differently from the same terms in the context of an allegation of vicarious liability. However, not all US courts follow the indication in the Congressional report. For example, in *Costar Group Inc. v. Loopnet, Inc.*, Judge Chasanow concluded "the DMCA provides no safe harbor for vicarious infringement because it codified both elements of vicarious liability".[98] In *Perfect 10, Inc v. CCBill, LLC*, the Ninth Circuit held "direct financial benefit should be interpreted consistently with the similarly-worded common law standard for vicarious copyright liability."[99] However, for most US courts, the statement in the legislative history seems a more reasonable interpretation and persuasive. For instance, in the appeal of *Costar Group Inc. v. Loopnet, Inc.*, the Fourth Circuit held that even though an ISP should undertake vicarious liability under common law, it "may still look to DMCA for safe harbor if it fulfilled conditions therein."[100] In a case closed in 2012, the Ninth Circuit also concluded that in some cases, ISPs subject to vicarious liability can be exempted from monetary remedies if they fulfill the requirements of the "safe harbor" provision, and specified that the "right and ability to control such activity" in DMCA 512(c)(1)(B) should be interpreted narrower than analogous terms under vicarious liability.[101]

As for what is the direct benefit in DMCA §512(c)(1)(B), according to the House Report, if an ISP principally runs a legal business and charges infringers the same fees as it charges non-infringing users, then the profit received by the ISP is not directly attributable to infringements.[102] Therefore, "receiving a one-time set-up fee and flat, periodic payments for service" from an infringer would not constitute direct benefits, nor would receiving fees "based on the length of the message or by connect time". However, "where the value of the service lies in providing access to

[97] H.R. Conf. Rep. No. 105-796, 73.

[98] *Costar Group Inc. v. Loopnet, Inc.*, 164 F. Supp. 2d 688, 704 (D. Md. 2001).

[99] *See Perfect 10, Inc v. CCBill, LLC*, *supra* note 28, at 1117.

[100] *Costar Group Inc. v. Loopnet, Inc.*, 373 F.3d 544, 555 (4th Cir. 2004).

[101] *See UMG Recording, Inc. V. Veoh Internet, Inc.*, *supra* note 32, at 1042–1045. In this case, the plaintiff UMG is a recording company which has copyright over considerable amounts of music, some of which was uploaded onto the defendant's running video-website Veoh, so the plaintiff sued Veoh for copyright infringement.

[102] *See* H.R. REP. 105-551(II), *supra* note 21, at 54.

infringing materials", the foresaid fees should be accounted as direct benefit.[103] In case law, besides referring to the Report above,[104] US courts also rely heavily on the standard of benefiting directly as developed under vicarious liability in common law, and thus base their conclusion on "whether the infringing activity constitutes a draw for subscribers, not just adding benefit".[105] Regardless of whether they follow the criteria stated in the House Report or the "constituting a draw" standard in common law, it is held that the defendant's hosting of websites for a fee was not sufficient to prove its receiving direct financial benefit from infringements.[106] However, charging fees based on offering a host service is only one way of making profits, and nowadays it is quite typical for a hosting ISP to offer a free hosting service, but to sell advertising space to generate profits, as Veoh, YouTube and other content-sharing websites do. This raises the question, therefore, as to whether the sale of advertising space can be identified as receiving a direct financial benefit from infringements. The US courts seem to avoid answering this question, but instead try to resolve the problem of hosting ISPs' qualifying for DMCA 512(c)(1)(B) by analyzing whether the hosting ISPs have the right and ability to control the infringements. This is because if a hosting ISP has no right and ability to control the infringements, then the court does not need to consider whether the hosting ISP receives direct benefit from infringements, and thus it certainly qualifies for DMCA 512(c)(1)(B). For instance, in *Io v. Veoh*, the Court held that "even assuming (without deciding) that Veoh received a direct financial benefit from the alleged infringing activity," since the "defendant does not have the right and ability to control such activity," the defendant still did not lose its qualification for DMCA 512(c)(1)(B).[107] In the first instance of *Viacom v. YouTube*, the Court admitted that "there may be arguments whether revenues from advertising, applied equally to space regardless of whether its contents are or are not infringing, are 'directly attributable to' infringements," but then based on YouTube's lack of right and ability to control the infringements, it then held that YouTube still qualified for the DMCA 512(c)(1)(B) safe harbor.[108]

[103] *Id.*

[104] *See Costar Group Inc. v. Loopnet, Inc.*, *supra* note 98, at 720. In this case, the court held that it would not be considered as a direct financial benefit "where the infringer makes the same kind of payment as non-infringing users of the provider's service".

[105] *See Perfect 10, Inc v. CCBill, LLC*, *supra* note 28, at 1117; *see Io Group, Inc. v. Veoh Internets, Inc.*, *supra* note 31, at 1150. This standard can be traced to the classic case of *Fonovisa v. Cherry Auction* (76 F.3d 259, p. 264 (9th Cir. 1996)). In this case, the 9th Circuit held that the sale of pirate recordings in a Cherry Auction swap meet is a "draw" for customers, so the defendant who ran this swap meet directly benefited from infringements.

[106] *Id*, *Perfect 10, Inc v. CCBill, LLC*, at 1118. In this case, the defendant, CWIE, hosted websites for a fee, and some of these websites included content which infringed the plaintiff's copyright. First, the 9th Circuit held that the defendant's hosting of websites for a fee was not sufficient to prove the infringements functioning as a "draw" in the context of vicarious liability. Further, by noting that "receiving a one-time set-up fee and flat, periodic payments for service from a person engaging in infringing activities would not constitute receiving a 'financial benefit directly attributable to the infringing activity'", the 9th Circuit held that the hosting fee received by the defendant was not directly attributable to infringements.

[107] *Io Group, Inc. v. Veoh Internets, Inc.*, *supra* note 31, at 1150.

[108] *See Viacom v. YouTube*, 718 F.Supp.ed 514, 517 (S.D. N.Y. 2010). In this case, the court held that in any event the provider must know of the particular case before he could control it. This interpretation of "control" has been overruled by the appeal court, which specified that "control" has nothing to do with hosting ISPs' "item-specific" knowledge of infringements. *See Viacom v. YouTube*, *supra* note 5, at 36–38.

When it comes to having the "right and ability to control infringement", nearly all US courts have held that the control provision in the DMCA 512(c)(1)(B) should be interpreted differently from the common law vicarious liability criteria, and that it "required something more than the ability to remove or block access to materials posted on a service provider's website".[109] The "something more" standard was derived from the "notice-takedown" mechanism in the DMCA because in order to conform to the "notice-takedown" mechanism, a hosting ISP must have the right and ability to remove or block the infringement complained of by the copyright owner.[110] Regarding what constitutes "something more", only a few US courts have made relevant statements. In *Perfect 10, Inc. v. Cybernet Ventures, Inc.*, which is the only case to conclude that an ISP has the right and ability to control infringement under the DMCA §512(c)(1)(B),[111] the court based its conclusion on the following facts: the defendant ran a monitoring program to notify service receivers with "detailed instructions regarding issues of layout, appearance, and content", and if a service receiver failed to comply with the instruction, its access to service would be blocked.[112] Two other courts suggested that the following conducts may fulfill the "control" requirement: (1) being "actively involved in the listing, bidding, sale and delivery" of items offered for sale;[113] and (2) controlling vendor sales by previewing products prior to their posting, editing product descriptions, or suggesting prices.[114] By examining the factors listed above, it can be concluded that US courts set a very high standard for the control provision in the DMCA §512(c)(1)(B), and consequently the normal hosting ISPs without being actively involved in choosing posted contents can hardly meet the threshold of "control". Furthermore, a hosting ISP which commits an inducing infringement is high likely to fulfill both elements of "control" and "direct benefits".[115]

[109] *See Viacom v. YouTube*, *supra* note 5, at 36–38. In this case, the court summarized all decisions about the control provision in the DMCA 512(c)(1)(B), and concluded that the prior case law completely agreed with the opinion that the control provision required something more than the "ability to remove or block" the hosted content.

[110] According to the "notice-take down" mechanism, once a hosting ISP receives a competent notice about infringing content, it should expeditiously remove or disable access to material alleged to be infringing. Therefore, the DMCA 512 has already implied that a qualified hosting ISP should have the right and ability to remove or disable access to materials posted on its website. A similar analysis can also be found in the relevant US case law. For example, in the case of *Hendrickson v. Ebay Inc*., the Court stated "Congress could not have intended for courts to hold that a service provider loses immunity under the safe harbor provision of the DMCA because it engages in acts that are specifically required by the DMCA." *See Hendrickson v. Ebay Inc.*, 165 F. Supp. 2d 1082, p. 1093–94. (C.D. Cal. 2001).

[111] *See Viacom v. YouTube*, *supra* note 5, at 38.

[112] *See Perfect 10, Inc. v. Cybernet Ventures, Inc*., 213 F. Supp. 2d 1146, p. 1173 (C.D. Cal. 2002). In this case, the Cybernet ran a web-service called "Adult Check", and the plaintiff, Perfect 10, was a corporation owning copyright over considerable pornographic content. During the hearing, the court was unsure about whether Cybernet was a qualified ISP. However, the court held that even with the assumption of Cybernet's qualification as an ISP, Cybernet could still not enjoy the shield of the "safe harbor" provision, because it failed to conform to the DMCA 512(c)(1)(B).

[113] *See Hendrickson v. eBay, Inc*.,*supra* note 110, at 1094.

[114] *See Corbis Corporation v. Amazon.com, Inc*., *supra* note 68, at 1110.

[115] The detailed discussion can be found in the following section "inducement liability in US".

To sum up, although the provision in the DMCA §512(c)(1)(B) can be seen as originating in vicarious liability in common law, it should be interpreted as being less strict when applied to hosting ISPs, because it is set to limit hosting ISPs' liability. Along this track, US courts mainly focus on defining which benefit is not directly attributable to infringement and which conduct is not a "control" rather than defining what constitutes direct benefits and "control". Therefore, hosting ISPs running a normal commercial model, such as Veoh, YouTube and Amazon, are still qualified for the DMCA §512(c)(1)(B).

### 5.2 Benefit in Germany

Whether a hosting ISP receives benefit from copyright infringement is not an independent culpable element in Germany, because neither the Telemedia Act Sec. 10 nor general tort law rules clearly forbid receiving benefits, but German courts do take it into account when deciding whether a hosting ISP should be liable for direct user infringement.

In Germany the courts can deem a hosting ISP as a content provider and thus directly liable for infringement ("*die Haftung als Content-Provider für eigene Inhalte*"). When deciding whether a hosting ISP should be treated as a content provider from a legal perspective, German courts always refer to the factor of receiving a benefit. For instance, in a case involving a platform for photograph exchange, the Berlin Court of Appeal concluded that the defendant ran the platform as a content provider, and one of the reasons was the defendant received 40 % of the fees paid by the users who downloaded the photographs, the rest of the fees being passed on to the users who offered those photographs for sale.[116] In another case involving the video-sharing website YouTube, the Hamburg District Court found that "YouTube commercially exploits the uploaded videos by selling ad space" as being one of the reasons to hold YouTube as a content provider.[117] However, only receiving benefit from infringing content cannot lead a hosting ISP to be liable, because the German Federal Supreme Court set a quite strict precondition to make benefit be imputed in the case *Marions v. Kochbuch*.[118] In this case, the German

[116] KG: *Internetplattform zum Austausch von Fotodateien*, 2010 *MMR* 204. The other three reasons are as follows: (1) in particular, the uploaded photographs went through a selecting and checking procedure before they were publicly accessible; (2) the copyright owners of the photographs were pointed out but in an unnoticeable and indiscreet way; and (3) in the front part of the website, the corresponding philosophy of the operator was displayed under its logo, which was "publish modern and time-spiritual photos".

[117] Hamburg District Court, *Haftung eines Plattformbetreibers – "YouTube"*, 2010 *MMR* 834. The other reasons are as follows: (1) the logo of YouTube appeared on the upper right corner of videos because of a pre-designed website frame, when the downloadable videos were on play, but by contrast the signs for pseudonym of the uploading-users were very small and appeared on a separate part of the website apart from the videos; (2) the defendant sorts the uploaded videos into different categories, and when a video is clicked, the similar videos will show up on the right side of the webpage automatically; and (3) YouTube requires the uploaders to grant it the right to use these videos.

[118] German Federal Supreme Court, *Verwendung fremder Fotografien für Rezeptsammlung im Internet – marions-kochbuch.de*, 2010 NJW-RR 1276–1278. In this case, the defendant operated a website called chefkoch.de for the public to upload cooking recipes and corresponding photographs and the plaintiff ran a website called marions-kochbuch.de which introduced cooking recipes with depicting pictures. The plaintiff found that some of his copyrighted cooking instructions had been uploaded to the defendant's website, so he launched a suit against the defendant for copyright infringement.

Federal Supreme Court emphasized that whether the defendant selected, checked, edited and integrated the uploaded contents into its website should be deemed as the core factors to conclude the defendant's liability as a content provider, and the other facts, such as requiring a right transfer and receiving benefit are only supportive evidences to conclude the liability.[119] By examining the decision of Federal Supreme Court, one finds that "*die Haftung als Content-Provider für eigene Inhalte*" is to some extent comparable to the DMCA §512(c)(1)(B) in the US, because integration of uploaded content into its website can be seen as having the right and ability to control infringement, and the benefit received by a hosting ISP through integrating infringing content into its website can definitely be seen as directly attributable to infringement.

### 5.3 Direct Benefit in China

Article 22 of the Regulation provides that a hosting ISP can be exempted from monetary remedy if it fulfills certain requirements, one of which is "not receiving benefit directly attributable to infringements". Since neither Chinese tort law rules nor Chinese copyright law categorized benefits as direct or indirect, the concept of "direct benefit" in Art. 22 was obviously introduced from the DMCA 512(c)(1)(B). However, for some unknown reason, the other element of "right and ability to control" was not integrated into Art. 22. Faced with this new concept of "direct benefit", Chinese courts seem to be unsure of how to interpret it, and some courts have even reached completely different conclusions when interpreting similar facts.

In China, the public is generally free to use most hosting services, so a hosting ISP will mainly make profits by selling advertising space on its website. This raises the question of whether this kind of benefit should be affirmed as directly attributable to infringements. In the case *BuSheng v. YoBo*, the Haidian District Court in Beijing concluded the existence of direct benefits based on the following analysis: the infringing music on the defendant's website attracted more people to visit its website, so the defendant could make more profits by selling advertising space.[120] In contrast, in another case *CiWen v. 56.com*, the Beijing Second Intermediate People's Court concluded that all of the videos on the defendant's website could be viewed for free, and although an advertisement was being displayed with a copyrighted work owned by the plaintiff, there was insufficient evidence to prove that the benefit received by the defendant in this case was directly attributable to this copyrighted work.[121] In limited instances, the court has concluded a hosting ISP's liability based on selling advertising space even without considering whether it constitutes direct benefit or not. For example, in the case *joy.cn v. 56.com*, the Haidian District Court held that, since the defendant 56.com

[119] *Id*, German Federal Supreme Court, at 1276.

[120] *BuSheng v. YoBo*, No. 6939 Hai Min Chu Zi(2008). In this case, the plaintiff BuSheng owned copyright of certain musical works, some of which had been uploaded to the defendant's websites by Internet users, so the plaintiff sued YoBo for copyright infringement.

[121] *CiWen v. 56.com*, No. 9 Er Zhong Min Zhong Zi (2008). In this case, a television series call "Jia" (Family) owned by the plaintiff CiWen had been uploaded to the defendant's website "56.com" without permission, so the plaintiff sued "56.com" for copyright infringement.

had profited by displaying advertisements with the uploaded content, it needed to undertake a higher level of duty of care to check for potential copyright problems among the uploaded content; however, the defendant had not fulfilled this kind of duty of care, so it should be held liable.[122] Furthermore, Art. 22 of the Regulation also requires hosting ISPs not to alter the works, performance, sound or video recordings that are provided by the service acceptors. Some Chinese courts have held that displaying advertisements with uploaded contents forms a sort of alteration in the context of Art. 22, and have thus expelled hosting ISPs from the "safe harbor". For example, in the case *joy.cn v. 6room.com*, the HaiDian District Court concluded that, since before and after the playing of alleged infringing videos, 6room.com displayed advertisements, and whenever a viewer clicked on the pause button, an advertisement would also appear, the defendant had actually altered the alleged infringing videos supplied by Internet users when it added advertisements.[123]

Today, however, Chinese courts no longer seem to treat "display advertisements" as an "alteration". According to a judicial guideline published by the Beijing Higher Court (hereinafter "Opinions"),[124] "displaying the advertisement before or after the playing of the works, performance, sound or video recordings, or popping up ads during the playing of the works, performance, sound or video recordings" should not be found as an alteration of uploaded contents.[125] Moreover, the latest Judicial Interpretation promulgated by the People's Supreme Court includes a detailed provision about what constitutes direct benefit, which states the following:

> Where service providers make profits by displaying advertisements along with specific works, performances or sound or video recordings, or receive other financial benefits which are specifically related to the works, performances or sound or video recordings transmitted by them, it should be concluded that the service providers receive direct financial benefits; however, the normal advertising fee or service fee collected by service providers on the basis of offering an Internet service cannot be identified as direct benefit.[126]

[122] *joy.cn v. 56.com*, No. 24750 Hai Min Chu Zi (2008). In this case, some copyrighted videos owned by the plaintiff "Joy.cn" had been uploaded to the defendant's website "56.com" without permission, so the plaintiff sued "56.com" for copyright infringement.

[123] *joy.cn v. 6room.com*, No. 22186 Hai Min Chu Zi (2008).

[124] This judicial guideline, called "Opinions of Beijing Higher People's Court on Several Issues Concerning Disputes about Internet Copyright Infringements (trial)" (hereinafter "Opinions"), is not a mandatory legal document, because unlike the People's Supreme Court in China, the Beijing Higher People's Court has no statutory rights to promulgate any judicial interpretation of general application. However, Beijing, as one of the two cities (the other is Shanghai) hearing most of the disputes about Internet copyright infringement in China, the courts there always take a lead in solving these disputes and have accumulated considerable judicial experience in this respect. Therefore, the judicial guideline provided by the Beijing Higher People's Court definitely has widespread influence in China and will be used as an important reference by other courts.

[125] *Id*, Art. 24(3).

[126] *See* Provisions, *supra* note 15, Art. 11.

Therefore, where selling advertising space is regarded as receiving direct benefits, a specific relationship should exist between advertisements and the content with which they are displayed. This kind of specific relationship indicates that service providers have a certain ability to control the uploaded content, since the service providers should specify the content before displaying any advertisement with it. Consequently, although the Regulation does not restrict "receiving direct benefits" with the element of "control", Chinese courts have already realized that "receiving direct benefits" should be interpreted strictly and that service providers should at least have some sort of control over the uploaded content when concluding that they directly benefit from selling advertising space.

To sum up, the US "safe harbor" provision requires a hosting ISP not to receive direct benefit from infringement when it can control the infringing activities. It seems that US courts interpret the "receiving direct benefit" prong by referring to vicarious liability in common law, but since the "control" prong has been quite strictly interpreted, in only a few cases have hosting ISPs been blocked from the "safe harbor" because of making profits through their services. In Germany, "receiving benefit" is one factor used to hold a hosting ISP liable as a content provider; however, after the *Marions v. Kochbuch* case was decided by the Federal Supreme Court, "receiving benefit" became merely supportive evidence, and whether a hosting ISP edits or integrates uploaded content became the deciding evidence. In China, although the Chinese "safe harbor" provision does not exert "hosting ISPs' ability to control infringements" as a restriction to the element of "receiving direct benefit", the "control" requirement has already been indicated in the Judicial Interpretation issued by the People's Supreme Court. Ultimately, in these three countries, a hosting ISP cannot be held liable because it simply operates a normal advertising business without choosing with which content the advertisements are displayed.

## 6 Inducement Liability

Since a service provider's liability cannot be concluded from its offering a service which is capable of substantial non-infringing use, the service provider's intent should be an important reference for courts in deciding its liability. This is because the "safe harbor" provision is not aimed at indulging copyright infringements. Therefore, if a service provider encourages or induces its users to commit infringements with illegal intent, then it is probably barred from the "safe harbor" provision and, thus, liable for primary infringements.

### 6.1 Inducement Liability in the US

In *Grokster*, the US Supreme Court adopted inducement liability into the field of Internet copyright against a p2p software company of the same name. Inducement liability can be concluded under either of these two circumstances: (1) "actively encouraging (or inducing) infringement through specific acts"; and (2) "distributing a product distributees use to infringe copyrights, if the product is not capable of

'substantial' or 'commercially significant' non-infringing uses."[127] As for the former circumstance, it can be further described as distributing "a device with the object of promoting its use to infringe copyright, as shown by clear expression or other affirmative steps to foster infringement."[128] After *Grokster*, several cases have addressed p2p software by taking advantage of inducement liability as established in *Grokster*,[129] but the relationship between inducement liability and the "safe harbor" provision was not substantially discussed until the *Fung* case.

In the first instance of *Columbia v. Fung*, the court held the defendant Gary Fung contributorily liable for inducement of copyright infringement on the following grounds: (1) the defendant's message to users demonstrated its consistent intent to promote the infringing use of its service, such as setting special pages for users to upload dot-torrent files involving top popular movies; (2) the defendant assisted its users in engaging in infringement; (3) the defendant implemented the technical measures to promote copyright infringement; and (4) the defendant's business model depended on massive infringing use.[130] When facing the defendant's assertion of its qualification for the "safe harbor" provision, the court stated "inducement liability and the Digital Millennium Copyright Act safe harbor are inherently contradictory." This is because inducement liability results from bad faith conduct with a purpose of promoting infringement, but the "safe harbor" provision aims at protecting the legal e-business run in good faith.[131] Therefore, the district court in *Fung* appeared categorically to bar inducement liability from the "safe harbor" provision.[132]

In the appeal of *Columbia v. Fung*, the 9th Circuit Court also started by comparing this case to *Grokster*, and then concluded that the defendant, Fung, had fulfilled every element of inducing infringement, including the distribution of a device or product, acts of infringement by Internet users with the object of promoting its use for infringing copyright, and causation between infringements and inducing. Hence, Fung needed to undertake inducement liability.[133] However, when addressing to the relationship between inducement liability and the "safe harbor" provision, instead of holding that inducement liability could be categorically

[127] *MGM Studios Inc. v. Grokster*, 545 U.S. 913, 942.

[128] *Id*, at 913.

[129] *Arista Records, LLC. v. Lime Group, LLC*, 784 F. Supp. 2d 398, 424 (S.D.N.Y. 2011). This is a case against p2p software, and since running a p2p software is not a typical Internet service covered by "safe harbor" provision, the court need not discuss the relationship between inducement liability and the "safe harbor" provision.

[130] *See Columbia Pictures Industries, Inc. v. Gary FUNG*, 2009 WL 6355911 (C.D. Cal.), 9–15. In this case, the defendant, Gary Fung, ran several websites which would "collect, receive, index, and make available descriptions of content, including so-called 'dot-torrent files,' and would also provide access to 'open-access' BitTorrent Trackers." Consequently, the district court denied treating the defendant's service as a transitory digital Internet communication or host rather than an information location tool. However, the court made a clear statement about the relationship between inducement liability and the "safe harbor" provision, so it is still relevant to the discussion here. Moreover, in the appeal instance, the 9th Circuit held that the defendant could be seen as a hosting ISP.

[131] *Id*, at 18.

[132] *See* Anthony Reese (2011).

[133] *See Columbia Pictures Industries, Inc. v. Gary FUNG*, 710 F.3d 1020, 1032–1037. (9th Cir. 2013).

excluded from the "safe harbor" provision, the 9th Circuit mentioned the possibility that a hosting ISP who committed inducement could still be shielded from liability.[134] However, the 9th Circuit still found Fung liable, because he failed to meet the "safe harbor" provision for host or information tools ISPs.[135] To be precise, Fung was "aware of facts or circumstances from which infringing activity was apparent," and received a benefit directly attributable to the infringing activity where he had the "right and ability to control such activity."[136]

The 9th Circuit held that the defendant had the "red flag" knowledge of infringement on the basis of his particular inducing activities; the record was "replete with instances of Fung actively encouraging infringement, by urging his users to both upload and download particular copyrighted works, providing assistance to those seeking to watch copyrighted films, and helping his users burn copyrighted material onto DVDs."[137] These materials were obviously copyrighted to a reasonable person and could not be "licensed to random members of the public" without any charge, because they were "sufficiently current and well-known".[138] Moreover, Fung also admitted that he had personally used the isoHunt website (one of the websites involved in this dispute) to download infringing materials.[139] Therefore, the 9th Circuit held that he had broad "red flag" knowledge of copyright infringement.[140] As for the "receiving direct benefit from infringement" prong of §512(c)(1)(B), the 9th Circuit based its holding on the following facts: (1) Fung attracted advertisers by pointing advertisements to the infringing materials; (2) Fung induced and assisted these persons who committed infringement on his websites so as to attract more visitors to his websites; and (3) Fung's revenue relied on the number of visitors to his websites.[141] Furthermore, the 9th Circuit also held that Fung had the right and ability to control the infringement, because:(1) Fung organized and described the torrent files on his websites so as to make these high-likely infringing materials much easier to access; (2) Fung assisted users in locating the likely infringing materials that they could find themselves; and (3) Fung personally removed disqualified torrents from his websites, such as fake or infected ones.[142] To sum up, even though the 9th Circuit refused to exclude inducement liability from the "safe harbor" provision categorically, a hosting ISP who commits an inducing infringement still seems to be high likely barred from the "safe harbor".

[134] *Id*, at 1040.

[135] *Id*.

[136] *Id*, at 1047. Quoting 17 U.S.C. §512(c)(1)(A)(ii), 17 U.S.C. §512(c)(1)(B), 17 U.S.C. §512(d)(1)(B), 17 U.S.C. §512(d)(2).

[137] *Id*, at 1043.

[138] *Id*.

[139] *Id*.

[140] *Id*. In this case, the 9th Circuit Court was still not entirely confident about "red flag" knowledge already being fulfilled, for the reason that it was uncertain whether exclusion from the §512(c) safe harbor because of actual or "red flag" knowledge of a specific infringing activity applied only with regard to liability for that infringing activity, or more broadly.

[141] *Id*, at 1045.

[142] *Id*.

### 6.2 Inducing Infringement in China

Hosting services are highly likely to be used for copyright infringement, so in order to prevent hosting ISPs from making more profits by promoting the infringing use of their services, Chinese courts tend to hold hosting ISPs liable if they commit certain inducements. The Provision issued by the People's Supreme Court reads that where service providers induce or encourage Internet users to infringe others' copyright by delivering words, offering technical support or rewarding credits, the service providers shall be concluded to have committed inducing infringements.[143] In addition, the Guide for Hearing Copyright Disputes Involving Video-Sharing (hereinafter "Guide") published by the Beijing People's Higher Court also provides that, where hosting ISPs, by taking advantage of their service models, induce or encourage Internet users to infringe the rights of others' works, performances, sound or video recordings on the Internet, the hosting ISPs shall be held to have committed inducing infringements.[144]

Only a few months after the Provision entered into force, a company which ran a bulletin board system (BBS) for Internet users to share content was held to have committed an inducing infringement in the case *chineseall.com v. 178.com*. In this case, the BBS operated by the defendant 178.com had a sub-platform for subscribers to upload ePub-formatted e-books, and a copyrighted book owned by the plaintiff had been uploaded without permission. The plaintiff sued 178.com for copyright infringement. According to the court investigation, the defendant had a policy of rewarding these subscribers who uploaded content or replied to such content with virtual "silver coins", thus the ChaoYang District Court in Beijing held that the defendant had induced its subscribers to commit infringements.[145]

By examining the Provision, the Guide, and the *178.com* case, one can see that Chinese courts have a stricter rule against hosting ISPs that commit inducements than do US courts. First, unlike the 9th Circuit, which rejected setting inducement liability as a categorical exclusion from "safe harbor", Chinese courts have already made it quite clear that an inducing infringement cannot enjoy the liability exemption provided in the "safe harbor" provision.[146] Second, even compared with the inducement liability criteria founded in *Grokster*, the Chinese inducing infringement is easier to reach, because *Grokster* required the defendant to induce infringements by clear expression or other affirmative steps,[147] whereas in China a general or even indirect inducement can lead a hosting ISP to undertake liability, such as awarding virtual "silver coins" to those subscribers who upload content or make comments.[148] Although the rule of inducing liability in China seems to offer better protection for copyright owners, it might also lead to the imposition of too

[143] *See* Provisions, *supra* note 15, Art. 7.

[144] Guide for Hearing Copyright Disputes involving Video-sharing (hereinafter "Guide"), Art. 3.

[145] *chineseall.com v. 178.com*, No. 8854 Chao Min Chu Zi (2013).

[146] In terms of the Provisions promulgated by People's Supreme Court, once the inducing infringement has been concluded, "safe harbor" provisions are not applicable anymore.

[147] *See MGM Studios Inc. v. Grokster*, *supra* note 127, at 913.

[148] *See chineseall.com v. 178.com*, *supra* note 145.

broad liability on the hosting ISPs. This is because for a hosting ISP running a service capable of both infringing and non-infringing use, any promotion of its service can be, in a broad sense, understood as inducing infringement. Therefore, it is better to limit the inducement to an active and specific action; otherwise, hosting ISPs would face too great a legal risk when trying new commercial models. In other words, only when a hosting ISP runs a commercial model that is based on infringement, and is also actively inducing its users to commit infringement, can it be held as a liable inducer. Moreover, even though the German courts have not set a particular rule concerning inducement liability, they also refer to hosting ISPs' intent and their commercial models when deciding how broad the hosting ISP's "disturber's liability" should be.[149]

It is worth noting that the same defendant, Rapidshare, faced different fates in two suits which occurred in the US and Germany, respectively. In these two cases, Rapidshare had operated an online hosting service for users to upload and share their content. While Rapidshare itself did not offer a search tool or index contents for users who wanted to search for specific materials, its users could still easily find the infringing materials on Rapidshare through search tools run by others.[150] In the US, the S.D. Cal. Court held that Rapidshare's commercial model was tolerable, and it neither committed contributory infringement nor needed to undertake inducement liability.[151] However, the same commercial model seems problematic in the view of the German Federal Supreme Court. It first held that Rapidshare needed to undertake "disturber's liability" because its commercial model substantially induced large-scale infringements.[152] Second, as for the scope of "disturber's liability", Rapidshare should exert comprehensive and regular control over its "link collections", such as seeking out any infringing "link collection" by taking advantage of general search machines such as Google, Facebook, and Twitter, and if necessary, proper web crawlers should also be used.[153] Nevertheless, although the courts in each jurisdiction have set different criteria regarding imputed inducement, there is a common tendency in these three jurisdictions that the courts take hosting ISPs' intent and commercial models as important factors when deciding liability.

## 7 Chinese Approaches to Resolving Hosting ISPs' Liability

In China, the People's Courts always resolve hosting ISPs' liability by referring to whether they have fulfilled reasonable duty of care in preventing Internet users from uploading infringing content. As for what kind of duty of care is reasonable for a hosting ISP, that remains unclear in Chinese judicial practice. However, it is at least certain that in the following two circumstances hosting ISPs should undertake a

[149] *See* what has been discussed in C(b) – "Störerhaftung – disturber's liability in Germany".

[150] *Perfect 10, Inc. v. RapidShare*, No. 09-CV-2596 H, 2 (S.D. Cal., 2010); *see* German Federal Supreme Court, *supra* note 79, at 1.

[151] *Id*, *Perfect 10, Inc. v. RapidShare*, at 6–11.

[152] German Federal Supreme Court, *supra* note 79, para. (b).

[153] *Id*, para. (c), para. 21.

higher level of duty of care when creating a channel for users to upload movies and television series, and when having famous works or hot-playing movies uploaded onto their websites.

### 7.1 Setting a Channel for Users to Upload Movies and Television Series

In order to make the uploaded content look well-organized, the operators of video-sharing websites always divide their uploading channels into different categories which are usually labeled with "original",[154] "movies and TV series", "entertainment", "education", "music" and others.[155] According to Chinese courts, the operators of video-sharing websites have the right to design the layout of their websites, but creating a channel specifically for movies and TV series is problematic. For example, In the case *nubb.com v. Tudou.com*, the Shanghai Higher People's Court concluded that since the defendant, Tudou.com, had set an uploading channel for "movies and TV series" parallel with a channel entitled "original", it must have known that the channel "movies and TV series" would induce a high possibility of infringement from occurring. Therefore, it should have undertaken more duty of care over the contents in the channel "movies and TV series" and was thus liable.[156] This raises questions as to how far this kind of higher duty of care can reach. Some courts have even interpreted it as monitoring liability. For instance, in the case *GuanShi Culture v. 6room.com*, the HaiDian District Court in Beijing concluded that the defendant, 6room, had created a channel especially for movies and TV series, which meant it obviously knew many professionally produced movies and TV series were being uploaded onto its website. Consequently, the defendant should have monitored the content being uploaded to the "movies and TV series" channel and thus was liable.[157] Interestingly, it is also common practice for video-sharing websites, such as YouTube and Veoh, to create different channels (including a channel for films) for Internet users to categorize their uploaded content, but US courts did not take this as a reason to require YouTube or Veoh to undertake a higher level of duty of care. Perhaps affected by the relevant US case law, the Provision (the latest Judicial Interpretation concerning settling disputes of copyright infringements over the Internet) does not specify that setting a channel for "movies and TV series" will result in a higher level of duty of care.[158] However, the Provision leaves considerable room for the lower courts to interpret in their own way.[159] According to the Guide

[154] The "original" here means the videos made by amateur Internet users rather than professional producers.

[155] This kind of division can be found on nearly all main video-sharing websites in China, such as "youku.com", "tudou.com", and "video.sina".

[156] *nubb.com v. Tudou.com*, No. 62 Hu Gao Min San (Zhi) ZhongZi (2008).

[157] *GuanShi Culture v. 6room.com*, No. 31332 Hai Min Chu Zi (2008). The HaiDian District Court also drew a similar conclusion in another case *GuanDianWeiYe v. Youku.com*, *see* No. 14023 Hai Min Chu Zi (2008).

[158] *See* Provisions, *supra* note 15.

[159] Articles 9 and 12 of the Provision list some instances where service providers should be concluded to "should know the infringements", and these two articles end with "other factors" to be considered, which leaves lower courts enough room to make their own judgments.

issued by the Beijing Higher People's Court, with regard to the involved works, performance or audio–videos found in the channel "movies and TV series", it is assumed that the defendants (video-sharing website operators) should know that these contents are infringing,[160] which means the operators of video-sharing websites still need to undertake a kind of duty of care similar to monitoring the channels of "movies and TV series".

### 7.2 Famous Works and Hot-Playing Audio–Video Works

For hot-playing audio–video works, the Chinese courts have not given a clear definition, but by deducing from case decisions, hot-playing audio–video works generally mean those movies and television series which are popular and are still playing at movie theaters or on regular television. Since in China the box office is still the main revenue source for most movie producers and that audiences who can watch the movies on the Internet might not pay to enter theaters, the Chinese courts require video-sharing websites to fulfill more duty of care so as to prevent hot-play movies from being uploaded. In the case of *vale.com v. Tudou.com*, the Shanghai First Intermediate People's Court held that because the production of movies was costly, it was almost impossible for copyright owners to make them available on the Internet for free; therefore, video-sharing websites should bear a higher level of duty of care with movies, especially for hot-play ones.[161]

As for what constitutes famous work, there is also no clear definition, which means courts must decide on a case-by-case basis. Once a work has been identified as being a famous work, a higher level of duty of care will be exerted on hosting ISPs. For instance, in the case *Hanhan v. Baidu*, the HaiDian District Court in Beijing first admitted that the defendant, Baidu, did not need to monitor the "Baidu Wen Ku" (a platform for Internet users to upload and share literature) operated by it. Moreover, when deciding whether the defendant should have known that an illegal copy of "Xiang" (a work copyrighted by the plaintiff) was being uploaded to "Baidu Wen Ku", the following factors were comprehensively considered: objectively accessing the current situation of "Baidu Wen Ku", the fame of Hanhan and his work *Xiang*, and Baidu's actual capacity to anticipate and control infringing activities. Finally, the Court concluded that the defendant should have exerted a higher level of duty of care on illegal copies of Hanhan's works, such as *Xiang*, because of Hanhan's reputation and the wide influence of his works.[162] By contrast, in the case *JiaHua Culture v. 56.com*, even though the defendant 56.com had created an upload channel called "movies and TV series", on the grounds that the movies shown were neither hot-play ones or famous in China, the ChaoYang District Court in Beijing held that the defendant was not liable.[163]

[160] *See* Guide, *supra* note 144, Art. 7(1).

[161] *vale.com v. Tudou.com*, No. 16 Hu Yi Zhong Min Wu (Zhi) ZhongZi (2009). In another case, *nubb.com v. Tudou.com*, the Shanghai Higher People's Court made a similar statement on protecting "hot-play movies", *see nubb.com v. Tudou.com*, *supra* note 156.

[162] *See Han Han v. Baidu*, *supra* note 85.

[163] *JiaHua Culture v. 56.com*, No. 20595 Chao Min Chu Zi (2013).

The Provision issued by the People's Supreme Court sets "the fame of works" as one of the factors to consider when concluding whether service providers should know about an infringement. Additionally, the Provision also includes rules regarding "hot-play audio–video works", which state that hosting ISPs shall be presumed to know of the existence of infringements in the following circumstances: where hot-play audio–video works are located on the homepages, other main pages, or other pages which can be easily accessed by hosting ISPs, or where hosting ISPs take the initiative to choose, edit, sort or recommend hot-play audio–video works, or set a special top list for them.[164] When examining these rules, they do not require hosting ISPs to undertake a higher level of duty of care than complying with the normal "red flag" test and not actively being involved in infringement. The Opinion published by the Beijing Higher People's Court also includes a similar provision, but it covers not only hot-play audio–video works, but also popular music, other types of works with a degree of fame, and the performances, sound or video recordings related to these famous works.[165] However, in terms of the Guide issued by the Beijing Higher People's Court, once hot-play audio–video works, performances, or sound or video recordings can be found on their websites, hosting ISPs can be presumed to know of these hot-play contents (and thus should be liable).[166] Therefore, by deducing from the Guide, hosting ISPs should monitor the hot-play content so as to avoid being held liable. To sum up, it is commonly held that hosting ISPs should thus exert a higher level of duty of care on preventing certain hot-play or famous content from being uploaded. However, when it comes to how high this specific duty of care should be, the People's Supreme Court does not require hosting ISPs to do more than simply comply with the "red flag" test, whereas the Beijing Higher People's Court asks hosting ISPs to at least monitor hot-play audio–video works, performances, sound or video recordings.[167]

## 8 Conclusion

Although the courts in US, Germany and China consider many common factors, such as knowledge of infringement, receiving benefits from infringements, taking necessary measures against repeat infringements, when concluding whether hosting ISPs are liable, the courts in each country still focus on their own preferences. In the US, the courts consider two main points, namely, whether the hosting ISPs fulfill the "red flag" test, and whether the hosting ISPs receive benefits directly attributable to infringements where they have the right and ability to control the infringing

[164] *See* Provisions, *supra* note 15, Art. 12.

[165] *See* Opinions, *supra* note 124, Art. 19(1). According to Art. 19(1), where the alleged infringing content includes hot-play audio–video works, popular music works or other types of works with good fame, or the performances and audio–video products, and this content is located on the homepages, other main pages or other pages which can be obviously accessed by service providers, then the hosting ISPs should be presumed to know about this infringing content.

[166] *See* Guide, *supra* note 144, Art. 8(1).

[167] The courts in Beijing have jurisdiction over most copyright disputes on the Internet, so the Opinion issued by Beijing Higher People's Court strongly affects cases about hosting ISPs' liability.

activities. In Germany, the courts mainly apply "disturber's liability", which concentrates on requiring the hosting ISPs to adopt reasonable measures to prevent the same infringing content from being uploaded again. In China, the courts mainly rely on "should know" criteria, which not only covers the US "red flag" test, but also aim at regulating the hosting ISPs' business model by requiring them to satisfy a certain duty of care. Nevertheless, some common tendencies can still be found by analyzing the case decisions in these three jurisdictions. First, "receiving benefits" as an imputed factor seems to have become less important than before. For example, in the US, with the restriction of having the right and ability to control infringing activities, hosting ISPs can barely be held liable even if they receive direct benefit from the infringements; in Germany, "receiving benefits" has already become a side-factor to be considered; in China, "receiving direct benefits" as an imputed factor can only be concluded under quite limited circumstances. Second, hosting ISPs' intent has become a more prevailing factor when the respective courts conclude liability. For instance, in the US, "willful blindness" and inducing infringement have been frequently discussed when the courts face cases involving hosting ISPs' liability; in Germany, if a hosting ISP induces copyright infringements to be committed on a substantial scale, compared with a regular hosting ISP without inducement, it needs to take significantly more comprehensive measures to stop the same infringements from occurring again; in China, a general inducement or even an indirect inducement can lead a hosting ISPs to be held liable. Third, the courts tend to evaluate hosting ISPs' business models rather than simply checking whether their services are capable of non-infringing use or not. Generally, if a hosting ISP's business model is more likely to result in infringements, it needs to take more effective measures to prevent said infringements. Furthermore, although a general monitoring responsibility is strictly prohibited from being exerted on hosting ISPs, a specific monitoring responsibility has been established in Germany, which works thus: once infringing content has been identified, the hosting ISP needs to monitor this specific content so as to prevent it from being uploaded again. In China, a similar kind of specific monitoring responsibility can also be found in the Provision and relevant cases, but the monitoring scope seems to be much smaller than that required by the German courts. Finally, compared with the US and Germany, China requires hosting ISPs to undertake a higher level of duty of care to prevent hot-play audio–video works and famous works from being uploaded, which can offer better protection for such highly valuable content.

## References

Anthony Reese R (2011) The relationship between the ISP safe harbors and liability for inducement. Stan Tech L Rev 8, para. 19

Barazza S (2012) Secondary liability for IP infringement: converging patterns and approaches in comparative case law. J Intell Property Law Pract 7:855

Fitzner J (2011) Von Digital-Rights-Management zu Content identification: neue Ansätze zum Schutz urheberrechtlich geschützter Multimediawerke im Internet: eine technische, ökonomische und rechtliche Analyse. Nomos, Baden-Baden, p 283

Hoeren T, Yankova S (2012) The liability of internet intermediaries—the German perspective. IIC 43:510
Leistner M (2012) Grundlagen und Perspektiven der Haftung für Urheberrechtsverletzungen im Internet. ZUM 731
Matulionyte R, Nérisson S (2011) The French route to an ISP safe harbor, compared to German and US ways. IIC 42:66
Nimmer D (2003) Copyright: sacred text, technology, and the DMCA. Kluwer Law International, Hague, p 358
Patry WF (2009) Patry on copyright, vol 21. Thomson West, St Paul, p 85
Spindler G et al (2008) Recht der elektronischen Medien: Kommentar. C.H. Beck, Munich, p 1530
Wang Q (2008) Infringement research on copyright of video-sharing website. Stud Law Bus 4:42–53