A Critical Review of China’s Approach to Limitation of the Internet Service Provider’s Liability: A Comparative Perspective

Wenqi Liu†
Department of Social Science, Zhejiang Shuren University, Shuren Road, Hangzhou, Zhejiang Province, 310015, P R China

Received 26 February 2011, revised 3 May 2011

In an information society, granting the Internet Service Provider (ISP) exemption from liability under certain circumstances is an important approach to strike a balance between the interests of the copyright holder, the ISP and the public. Although many countries conditionally provide safe harbour protection for online services, the certainty, feasibility and efficiency of the relevant provisions are different from one country to another. This article reviews China’s approach to limitation of the ISP’s liability from a perspective of legislation and judicial practice, compares differences in this context between China, the US and EU, and based on which discusses the feasible options for China to increase the certainty of law and inconsistency in judicial practice.

Keywords: Internet service provider, liability, safe harbour, notice-and-takedown procedure

The advent of Internet in the 20th century encourages the robust development of communication, commercial transaction, research and education. People have recognized its vital role in view of the fact that the whole society increasingly relies on abundant information and high efficiency produced by the Internet. Likewise, the Internet has brought a substantial impact on copyright protection. On the one hand, the Internet serves the objective of facilitating information dissemination; and, on the other hand, poses a threat to right (owners’ control over their copyright) since intellectual creations can be easily accessed by illegal means through the Internet. The Internet Service Provider (ISP), playing a dominating role in cyberspace, is expected to act as a supporter of promoting the robust development of the cultural industry rather than a contributor to copyright infringement. Considering that imposing excessive duty on ISPs does not benefit the growth of the Internet industry,1 countries endeavour to strike a balance between the interests at stake by limiting the liability of ISPs in case copyright infringement is directly attributable to third parties.2

In order to strengthen copyright protection over the Internet, the Copyright Law of China enacts the right to network dissemination of information, granting right owners an exclusive right to permit or prohibit public access to their works by wire or wireless means at the individually selected time place [Article 10(12)]. Moreover, the Regulations on the Protection of the Right to Network Dissemination of Information (RNDI) released by Chinese State Council, details provisions regarding fair use in the network environment and liabilities of ISPs.3 In addition, the Interpretation of the Supreme People’s Court on Several Issues Concerning the Application of Law in the Trial of Cases Involving Copyright Disputes over Internet has been issued to achieve a uniform understanding in dealing with such cases.4 However, the rough and vague language residing in relevant provisions generates ambiguity and inconsistency in judicial practice. In consequence, it is substantially necessary to clarify problematic issues and thereby make the copyright legal regime more predictable and practical. This article does not discuss cases in which ISPs directly conduct infringing activities, but focuses on the circumstances under which an ISP can be granted immunity from liability. Also, (i) it analyses the absence of definition of an ISP and its potential effects in Chinese copyright regime; (ii) reviews the liability limitations for ISPs from a perspective of legislation and judicial practice and compares differences between China, the United States and countries of European Union (EU); (iii) studies the notice-and-takedown procedure; and, based on the aforesaid discussion, (iv) finally, concludes that endeavours by the legislature and courts are needed to improve the certainty and feasibility of the system of ISP’s liability limitation.

†Email: wenqiliu@gmail.com
Definition of an ISP

Commonly, ISP refers to an entity that provides its customers with connection to the Internet and other kinds of services in cyberspace. The extended scope covers both ISPs who offer Internet access or WAN facilities and ISPs who acquire or transmit information, including editorial and multimedia contents through Internet.

In the US, the Digital Millennium Copyright Act (DMCA) divides ISPs into two categories. The first category means entities ‘offering transmission, routing, or providing connections for digital online communications, between or among points specified by a user, of material of the user’s choosing, without modification to the content of the material as sent or received.’ They merely act as a data conduit on the network, through which digital information is transmitted from one point to another upon the users’ request. The second type refers to the providers of ‘online services or network access, or the operator[s] of facilities,’ [Section 512 (k)(1)(b)] which at least involves the services of system caching, information storage, and information location.

The Directive on Electronic Commerce of EU (e-Commerce Directive) defines the ‘service provider’ as ‘any natural or legal person providing an information society service.’ Information society services include ‘any service normally provided for remuneration, at a distance, by means of electronic equipment for the processing (including digital compression) and storage of data, and at the individual request of a recipient of a service’ (Article 22, preface). This broad definition covers various means of digital data transmission, including Internet services.

Unfortunately, no clear definition of the ISP can be found in Chinese legislations. Despite the provisions concerning the right to network dissemination of information and the liability of ISPs, the copyright law and related regulations seemingly neglect to offer a precise definition for the ISP. Although the RNDI mentioned several types of Internet services in separate articles, including automatic transmission, information storage, search engines and hyperlinks, the absence of a clear definition not only causes uncertainty of the law, but allows little room for encompassing new types of ISPs in the future. This problem has been addressed in some cases. For example, in Ciwen Ltd v Wangtong Hainan Ltd, the court divided ISPs into two categories: one providing connecting service, and the other providing content service. Meanwhile, the court ruled that because the latter has a stronger ability of control over the Internet information than the former, the obligation and liability of the two types of ISPs should be different. It should be noted that precedents will not necessarily bind future cases in China; therefore, the legislation or judicial interpretation offered by the Supreme Court will be more helpful for providing a uniform understanding. In fact, the DMCA or the e-Commerce Directive provides a good precedent to follow in view of the clear and broad description of an ISP.

Limitation on Liability of an ISP

Considering that the ISP usually plays a passive role in copyright infringement in cyberspace, it is sensible to treat the ISP differently from the entity that directly conducts infringing activities in terms of duty of care and liability. In a welfare society, the country has a duty to ensure dissemination of information as well as protect intellectual creations.

In order to explore an equitable system for balancing the interests of stakeholders and ensure that such a system would not unfairly hinder the development of Internet industry, copyright laws of countries impose limitations on the liability of ISPs for monetary relief (safe harbour). Overall, countries do not impose a general obligation on ISPs to monitor the material which they transmit or store, nor require ISPs to seek facts indicating illegal activity. However, there are still some differences among countries on specific conditions of liability limitation, such as standard of ‘red flag’, understanding of technical terms, attitude to injunctive relief, and so on. For example, some countries adopt a very strict standard for proving the illegal intent of ISPs, which makes it easy for ISPs to enjoy the protection under safe harbour.

ISPs for Transitory Network Communications

China provides liability limitations for ISPs offering services of mere connection. It can be said that Article 20 of the RNDI is a simplified version of Section 512(a) of the US Copyright Act. According to it, the ISP that provides services of automatic access or transmission upon the request of its subscribers is exempted from monetary liability, on the condition that they do ‘(1) not select or modify the transmitted work, performance, sound or video recording; and (2) provide the work, performance, sound or video recording to the designated recipient, and prevent other persons other than the designated
recipient from accessing these materials.’ Even though the legislature attempts to achieve a similar effect as the DMCA by using this clause to limit the ISP’s liability, there are at least two defects. First, the absolute expression concerning the duty of preventing infringement imposes an excessive burden on the ISP. From the literal understanding, the expression of ‘prevent other persons other than the designated recipient from accessing these materials’ does not involve any consideration about whether the ISP has fulfilled the general duty of care. Under the DMCA, the corresponding duty of the ISP is: (1) not maintaining a copy of the transmitted material on its system in a manner that allows a third party to ordinarily access this material, or (2) maintaining it for an unreasonably long term as for the process of transmission, routing, or connection. It limits the scope of the ISP’s duty by using the wording ‘on its system’, ‘ordinarily’ and ‘unreasonably long term’. Actually, only if the ISP prevents persons other than the designated recipient from accessing these materials in an ordinary manner, should the ISP be immunized. Therefore, when a third party takes an un-ordinary measure to obtain the transmitted digital information, the ISP is not liable. Second, it is unclear whether this article grants permission of automatic, intermediate and transient storage of the transmitted material for the sole purpose of implementing data transmission. Once disputes concerning information storage in the process of data transmission arise, the settlement will depend on the interpretation by the court in the absence of specific provisions. With respect to this issue, the e-Commerce Directive in its Article 12(2) provides a good example, under which the automatic, intermediate and transient storage of the transmitted material for a unique purpose of implementing data transmission is allowed on the condition that such storage is maintained for a period no longer than that reasonably necessary for the transmission.

The liability limitation does not exclude the possibility that the court may grant injunctions against the ISP where the court or other authorities find that repeated infringing activities have been conducted by a subscriber who is using the connection service offered by that ISP. Although countries hold divergent views on granting injunctions to order the ISP to terminate the account of its subscribers for the purpose of preventing infringing actions, some countries have presented a positive attitude towards such an injunctive relief. A typical representative of the radical group is the US. The DMCA stipulates that the injunction may be issued, under which the ISP must terminate the accounts of ‘a subscriber or account holder of the ISP’s system who is using the provider’s service to engage in infringing activity,’ or the ISP is prohibited from providing access to ‘a specific, identified, online location outside the US’ (Section 512 (j)(1)(B)). This provision does not indicate that the court must do so, but that is also a possibility. Subject to such a provision, the court may make a decision based on a comprehensive consideration, case by case. Besides, the e-Commerce Directive expressly states that the liability limitation on mere conduit should not affect the possibility of a court or competent authority of a member country from ordering the ISP to terminate or prevent an infringement. This means that it leaves much room for the member country to decide its legislative system, i.e., whether its court or administrative authority can issue injunctions to order the ISP to terminate the connection service to its subscribers. France has taken one step towards this anti-piracy measure, wherein a specific administrative authority takes charge of dealing with the infringement complaints from the right holders and forwarding the related information to the appropriate ISP for action. The action to be taken by the ISP, namely ‘three strikes and you are out’, makes its subscribers who illegally use copyrighted materials face the loss of access to service. In detail, once the infringing activity of the subscriber is identified, the ISP will send a warning message and require him/her to cease the illegal behaviour at the first instance. In case the subscriber continues to behave in an infringing manner, the ISP will send the second warning message, which may result in suspension of access to service. If this subscriber is found to conduct infringing action again, the ISP will terminate the service. To some extent, this measure is of significance especially to fight against casual piracy. Additionally, it seems an appropriate penalty for illegal file-sharing done by young people rather than large fines and years in jail. Therefore, it cannot be denied that this means is substantially effective for enforcing copyright protection on the Internet.

**ISPs for System Caching**

China has a safe harbour for automatic system caching. Under the RNDI, the ISP can be immunized from liability of damage, where for the purpose of
improving the efficiency of information transmission, the ISP automatically stores a work, performance or sound or video recording obtained from other sources, and automatically provides such materials to its subscribers based on a technical arrangement, and the following conditions are satisfied: (1) not modifying the work, performance or sound or video recording that is automatically stored; (2) not influencing the original information provider who offers the work, performance or sound or video recording to collect the information on the subscribers’ access of these materials; and (3) whenever the original provider updates, removes or blocks access to the work, performance or sound or video recording, it takes corresponding action in line with the technical arrangement (Article 21). This article is in general similar to the provisions under the DMCA [Section 512 9b)] and e-Commerce Directive (Article 13), especially as to the requirements of no modification, no influence, and being subject to the technical arrangement. All of them indicate that the ISP can be shielded from liability only if its activity has a mere technical, automatic and passive nature and provided it does not control the cached material.

However, China’s stipulation does not require the ISP to expeditiously take measures to stop infringement upon the knowledge of the infringing action. It would be unfair to let the ISP enjoy the immunity when it has recognized the infringed material available in its system but turned a blind eye to the fact. Differently, as for this issue, the DMCA sets a specific condition of liability limitation for system caching that the ISP should expeditiously remove, or disable access to the claimed material upon notification of claimed infringement [Section 512 (b)(2)(E)]. In other words, if the ISP fails to fulfill the obligation of expeditious removal, it cannot enjoy the protection of safe harbour and may be liable for copyright infringement. Similar to the DMCA, the e-Commerce Directive stipulates the obligation of expeditious removal as a prerequisite of liability limitation for system caching as well.

Besides, it is worth discussing whether the liability limitation of the automatic system caching described in Article 21 of the RNDI can be applied to Peer-to-Peer (P2P) caching. P2P technology has been widely used in the Internet and greatly improved the efficiency of data transmission. Accordingly, the rapid development of P2P technology has had a deep impact upon copyright law. Generally, there is no debate that the system caching mentioned in the clauses of ‘safe harbour’ includes web caching. However, whether it also applies to P2P caching has not yet been addressed by the legislature or courts. Like web caching, P2P caching works well for accelerating transmission through the network. In line with a specific calculating method, P2P caching temporarily stores a copy of popular material on the ISP’s server. When the cached material is requested by the next user, P2P cache either serves the file directly or passes the request on to a remote peer. P2P caching dramatically increases the speed of information transfer since end-users usually obtain the copy of the requested material from the ISP’s local computer instead of from a distant peer. In order to analyse whether the liability limitation covers P2P caching, it is necessary to evaluate the differences between P2P caching and web caching in the first place. The ISP offering P2P service intends to distribute a copy of the requested material to the end-user, but the ISP of web service does not. For web caching, a temporary copy of a file is put into a cache of the ISP’s system for improving the speed of acquiring information. When an end-user browses a file online, a copy of the file is stored in the temporary dictionary of the user’s local computer, which is a hidden process. The record in this temporary dictionary will be automatically removed after a period in accordance with the system setting, provided that the end-user does not intervene with this automatic process. Therefore, the whole process of data acquiring and web browsing does not imply that the ISP intends to distribute a permanent copy of the file to the end-user. Nonetheless, P2P caching is a different story. Apparently, the P2P service provider even after recognizing that the goal of most end-users using P2P service is to download a copy from its local server, still serves such a goal. Furthermore, there is an essential difference between the two kinds of caching with respect to the ability of responding to changes of the original material. The provisions offering shelter from copyright infringement for system caching require the ISP to automatically and expeditiously change, remove or disable access to the material it has stored complying with the protocols such as update, removal or disablement set by the person who provides the original material online. It is easy for the ISP to realize it, but not in the P2P case. Once a cached copy of a file is put on the P2P server, this copy will exist all along unless it is deleted by the
ISP. Even if the original material is modified by the initial provider, P2P caching cannot automatically produce a corresponding response, except cache a new copy of the new version. In this situation, the original information provider has little interaction with either the file or the use. From this point of view, the nature of P2P caching is sharply different from ordinary system caching. Therefore, it is not logical to consider P2P caching the same as system caching when applying the rule of liability limitation under the current laws. In fact, in Verizon, the court distinguished system caching and P2P caching when analysing the application of subpoena because the court believed that ‘the legislative history of the DMCA betrays no awareness whatsoever that Internet users might be able directly to exchange files containing copyrighted works...The P2P software was not even a glimmer in anyone’s eye when the DMCA was enacted.’ However, it did not mention whether the Section 512(b) of the DMCA can be applied to P2P caching. Likewise, there is little discussion about it in China. But, unlike in the US, P2P technologies have been widely used when the RNDI was released. In consequence, it cannot be said that legislature is expected to give a detailed explanation in this context to promote certainty and predictability of the law.

ISPs for Hosting

Article 22 of the RNDI shields the ISP from liability of damage for hosting on the following conditions that: (1) it clearly identifies that the information storage space is provided for its subscribers, and publishes the name, contact person and web address of the ISP; (2) it does not modify the work, performance or sound or video recording provided by its subscribers; (3) it does not have actual knowledge and does not have reasonable grounds to know that the work, performance or sound or video recording provided by its subscribers is infringing; (4) it never directly receives a financial benefit from the work, performance or sound or video recording provided by its subscribers; and (5) in accordance with the RNDI, it removes the material claimed by the right owner upon receiving notification of the right owner (Article 22). In this issue, China’s provision is similar to e-Commerce Directive, but the latter seems much simpler, and only mentions two prerequisites, namely no actual or attributed knowledge of the infringing activity and the obligation of promptly removing the claimed material. Thus, EU’s e-Commerce Directive provides flexibility to its member countries to detail the condition of liability exemption. In comparison, China’s stipulation seemingly derives from Section 512(c) of the US Copyright Act, which grants an explicit safe harbour to the ISP providing service of information residing on its system at the direction of users. Both of them involve several essential elements when deciding liability exemption for hosting, such as not modifying the original material, no actual or attributed knowledge of the infringing activity (the red-flag test), no economic benefit from the claimed infringement, rapid removal of the claimed material, and so on. Nevertheless, the courts of the US and China have different opinions on the specific understanding of these elements, which will be discussed later.

Modification of Material

One condition of immunizing the ISP for hosting, not modifying the material provided by its subscribers, needs an accurate description. The reason of setting this requirement is to exclude the ISP doing more than merely providing a storage space from protection under the safe harbour. However, the word ‘modify’ does not include any changes of the original material arising due to automatic modification occurring in automated technological systems inevitable in the Internet world. The merit of the Internet lies in its ability to deal with enormous content in an automated process, so it is dangerous to echo any argument against its automated features that are fundamental to the Internet usage. The US’s courts have contributed to clarifying the contours of this issue. A good example is UMG v Veoh. In this case, UMG argued that Veoh did not fall within the DMCA safe harbour because Veoh converted each video into a flash format and separated some of the videos into smaller pieces in order to make them more manageable. The court rejected UMG’s argument by asserting that Veoh’s automated conversion only involves the form and ‘not the content of the movies.’ The same opinion was proposed by the court in Io Group v Veoh Networks, where the court ruled that ‘Veoh has simply established a system whereby software automatically processes user-submitted content and recasts it in a format that is readily accessible to its users.’ Unfortunately, in China, neither the RNDI nor the Supreme Court has interpreted the word ‘modify’. However, the Higher Court of Beijing has expressly excluded some
situations from the scope of ‘modifying’ the uploaded material as stated in Article 22 of RNDI, namely, merely modifying its storage format, adding the logo of the website or adding advertisements to it. The Higher Court of Beijing holds that the wording ‘modify’ means substantial changes to the original material, which implies the actual control over the claimed material.

**Actual or Attributed Knowledge**

It is also substantially important to elaborate the concept of ‘actual knowledge’ and ‘reasonable grounds to know’. There is little ambiguity in the actual knowledge criterion, since it is well accepted that ‘actual knowledge’ means the ISP actually knew about the infringing activities. But, the standard of constructive knowledge is different from one country to another. Regrettably, the RNDI offers little explanation.

The e-Commerce Directive provides a similar provision with respect to granting ISPs immunity from liability in the absence of actual knowledge and attributed knowledge [Article 14(1)(a)]. As for the former, the e-Commerce Directive adopts a subjective test, which requires that the condition of not having actual knowledge is fulfilled only if the ISP itself was not aware of the infringing activity. The e-Commerce Directive itself does not express under what circumstances and to whom the claimed infringement is ‘apparent’. However, the objective test addressed by UK case law can be taken here as an example. In *LA Gear Inc v Hi-Tech Sports PLC*, Morritt J conducted a ‘reasonable man’ test, and ruled that ‘it seems to me that ‘reason to believe’ must involve the concept of knowledge of facts from which a reasonable man would arrive at the relevant belief. Facts from which a reasonable man might suspect the relevant conclusion cannot be enough.’

Especially, Morritt J held that period of time should be allowed to enable a reasonable man to evaluate facts and thereby achieve a reasonable belief. This approach was also approved by the court of *Pensher Security Door Co Ltd v Sunderland City Council*.

Likewise, the DMCA exempts the ISP from liability if ‘in the absence of such actual knowledge, [it] is not aware of facts or circumstances from which infringing activity is apparent’ [Section 512(c)(1)(A)]. In the US, a high and strict standard is developed to explain the wording ‘apparent’. According to the Senate and the House Committee Report, ‘infringing activity is apparent’ (so-called ‘red flags’) means that the illegal activity is obvious ‘from even a brief and casual viewing.’ Setting such a high threshold for awareness of infringement is based on the consideration that it would upset the balance of interests among stakeholders if imposing an undue burden upon the ISP to require the ISP’s endeavours to differentiate what constitutes infringement and what does not. The Committee Report gave an explanation for this policy: ‘The commonsense result of this ‘red flag’ test is that on-line editors and catalogers would not be required to make discriminating judgments about potential copyright infringement. If, however, an Internet site is obviously pirate, then seeing it may be all that is needed for service provider to encounter a red flag.’

In judicial precedents, the courts of the US elaborated this policy. A representative case is *Perfect 10 v CCBill*, in which the defendant provided webhosting services to other websites that had copyrighted photos of the plaintiff without its permission. The plaintiff asserted that the copyright infringement was apparent on grounds that the domain names of two websites, to which the defendant offered hosting services, contained ‘illegal.net’ and ‘stolencelebritypics.com’ respectively. However, the Ninth Circuit rejected this argument by ruling that the domain names themselves did not constitute copyright infringement and such domain names might be used to increase attractiveness of the website, rather than an admission that the infringing contents are actually contained there. Moreover, the court held that under the DMCA, the ISP should not be placed the burden of determining whether the alleged contents are actually illegal. Another leading case, *Corbis Corp v Amazon.com*, followed a similar approach. In this case, the court rejected the plaintiff’s assertions that Amazon had known the existence of red flags based on its general awareness that infringing activities might be involved on its zShops sites, and explained that ‘merely being aware of one or more well known photographs of a celebrity at a site does not provide a service provider with knowledge of possible infringement.’

In China, the legislature and the Supreme People’s Courts have not provided the criterion of ‘reasonable grounds to know’ stipulated in Article 22 of the RNDI. In the absence of the standard of the red flag test, the courts developed different approaches in judicial practice. In *IFPI v Baidu*, Baidu was held not liable for copyright infringement, partly because
the Court believed that Baidu neither had ‘actually knowledge’ nor ‘reasonable grounds to know’ the infringing fact, by reasoning that the take-down notification provided by IFPI was not detailed enough to accurately locate the alleged infringing material. In another key case, Xingzhuan v Tudou, the court held a more liberal opinion concerning the red flag test. In this case, the defendant was a prominent hosting ISP in China; and the plaintiff, Xingzhuan was the copyright holder of a hit film –‘Crazing Stone’. Xingzhuan asserted that Tudou provided online service of playing this film without its authorization. However, Tudou argued that it had no knowledge or reasonable grounds to know that the infringing material was stored in its system, because all the material at the website of Tudou was uploaded by users, and it had not received any notice of removing the claimed material. The court of the first instance held that although the plaintiff did not send the notification to Tudou, the defendant, as a professional website, should have a general knowledge about contents that more likely involved infringing activities. Especially as for a hit film, the defendant should be aware that the contents entitled the same as the hit film would inevitably involve copyright issues. In other words, the court believed that in this case, Tudou has attributed knowledge of the infringing fact. Hence, Tudou was held liable for joint copyright infringement. After the first instance, Tudou brought an appeal to argue that the court of the first instance imposed an excessive burden upon it since it was impossible for an ISP to be aware of infringing activities in cyberspace based on limited information. The Appeal Court dismissed the Tudou’s appeal by ruling that the appellant had reasonable grounds to know the alleged video, ‘Crazing Stone’, was infringing. In the reasoning, the court stated that the appellant’s constructive knowledge of infringing activities could be observed from the following aspects. First, the appellant established separate channels, namely ‘original’, ‘film and TV’, ‘entertainment’ and ‘music’, for uploading different kinds of files. Separating the channel of ‘original’ from other channels indicated that the appellant had been aware that its subscribers might upload infringing materials other than original works in its server. Second, the appellant assigned a team of censors to take charge of reviewing the uploaded material before making it available online. In consequence, the appellant had the ability to find that the alleged video was illegal. Third, when the infringing video was opened online, people could read the digital watermark of the appellant’s logo on the video window, which verified that the claimed video had passed through the review process. Fourth, since ‘Crazing Stone’ was a hit film, Tudou should have common sense to know that the uploaded video with the same name was not unauthorized by the right owners.

Nonetheless, the court’s reasoning and conclusion in Xingzhuan v Tudou is highly contentious since it puts the ISP in a dangerous position with an obligation to seek out copyright infringement. Setting separate channels for different contents is an ordinary service offered by the hosting provider. Non-original works are not the same as illegal works. Providing a special hosting channel for original works does not indicate that the ISP allows illegal activities to take place in other hosting channels, or imply that the ISP has known or has reasonable grounds to know the copyright infringement. That an ISP generally knows that copyright infringement might take place on its site is not enough to meet the requirement of actual knowledge or constructive knowledge. Moreover, the pre-review system does not establish such knowledge as well, since it usually involves a general review on whether the materials transmitted by subscribers are morally harmful, offensive, or politically dangerous. It is impossible for the ISP to differentiate potential infringement through the pre-review process. Supposing that a conclusion can be drawn that the ISP can obtain the knowledge of copyright infringing facts from a general pre-review, the ISP would not like to conduct any censor or review any more. Furthermore, adding the digital watermark to each video is carried out through an automatic technical process rather than manual process. It is ludicrous to conclude that the ISP has actual knowledge or constructive knowledge of the infringing contents from the digital watermark of its logo showed on the video window. In addition, even though the alleged video involved a hit film and the uploaded material was titled the same name as the alleged hit film, the copyright infringement is not apparent from only viewing the title because of the fact that the files containing totally different contents often have identical names in cyberspace and an ISP has no duty to investigate further under the current legal system.

Despite the inconsistency of courts’ opinions, it cannot be ignored that the Directive Opinions (I) on Several Issues Concerning the Trial of Cases
Involving Copyright Disputes in Cyberspace (for Trial Implementation) (Directive Opinions of Beijing’s Higher Court) offers further interpretation concerning this issue. According to Article 19, an ISP providing information on hosting service may be determined to be at fault, if the alleged infringing contents stored are audio-visual works in current season and placed in locations obvious to the ISP, and the ISP fails to take measures to remove them within a reasonable period of time, or the ISP conducts any selection, organization or classification of the alleged material. These rules provide clear instructions on the standard of red flag; however, it does not bind all courts in China.

Financial Benefit

Under both the RNDI and the DMCA, not directly receiving a financial benefit from the alleged material is another prerequisite for liability limitation (Section 512 (c)(1)(B)). Hosting services involve plenty of financial benefits or financial interests, such as advertising fees, standard fees for service, increase of attractiveness of the site, and so on. Therefore, it is crucial to define the concept of ‘directly receiving an economic benefit’. In the US, the legislative authority and the courts have provided several explanations for it, and thereby have strict standards in order to limit the scope of this concept. However, in China, the RNDI itself does nothing about it.

In the US, the Congress used the words ‘receive a financial benefit’ in the DMCA instead of ‘have a financial interest’ traditionally used in the vicarious liability standard, on the grounds that the Congress aims at setting a high standard of an actualized liability standard, on the grounds that the Congress aims at setting a high standard of an actualized financial benefit. As for vicarious liability, the ISP’s business model of boosting advertisement and revenue by sharing copyrighted works may demonstrate financial benefits from infringement. But, the phrase ‘a financial benefit’ in the safe harbour provision refers to the benefit actually obtained by the ISP. Although the ISP may financially benefit from the copyright infringement, it does not amount to receiving a financial benefit. Besides, the DMCA requires a close causal connection between the financial benefit received by the ISP and the infringing activity. The court in Costar v LoopNet applied a strict standard for a financial benefit directly attributable to the infringing activity. In Costar, the district court held that ‘enhance[ing] the attractiveness of the venue to potential customers’ cannot be considered to qualify for financial benefit as stipulated in the DMCA, and that it was merely an indirect benefit. In CCBill, the Ninth Circuit stated 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.’

China’s courts have recognized that the court should be wary of a broad interpretation with regard to the financial benefit standard when applying the rules of safe harbour. In Longyue Ltd v Wangluoxiu Ltd, Longyue argued that Wangluoxiu received a financial benefit from the alleged material by charging for advertisement on its website. But, the court rejected this charge by reasoning that the definition of ‘a financial benefit’ should be explained narrowly, and such a financial benefit the ISP obtained should be directly attributable to the infringing activity. Therefore, the court held that mere advertising fee could not constitute a financial benefit from the alleged material; however, it would have been a different story if Wangluoxiu had charged for the uploaded material. This opinion was affirmed by the appeal court. Furthermore, the Directive Opinions of Beijing’s Higher Court narrowed the scope of ‘a financial benefit’ by excluding some kinds of financial benefits from the eligible financial benefits under the RNDI. Article 25 of the Directive Opinions of Beijing’s Higher Court stipulates that neither the standard fee from users as per time, flow, etc. nor the advertising fee charged by an ISP for the information storage space shall be considered as direct economic interests from the alleged material mentioned in the RNDI.

ISPs for Search Engines or Hyperlinks

Article 23 of the RNDI exempts the ISP providing service of search engines or hyperlinks from the liability of damage, provided that ‘it removes, complying with the RNDI, the links to infringing copies of a work, performance or sound or video recording upon receiving a notice from the right owner’ (as in Article 22). In Fanya v Baidu Wangxun, the court applied this article in its reasoning. Because no evidence could prove that Baidu Wangxun had actual knowledge or attributed knowledge of infringing activity, and Baidu Wangxun had expeditiously disabled access to the claimed material after receiving a notification from the plaintiff, the defendant was held not liable for the alleged damage. Moreover, the latter part of Article 23
stipulates the ISP’s joint liability where the ISP has actual knowledge or has reasonable grounds to know that the linked contents are infringing (as in Article 22).

However, the language of this article leaves loopholes. The article only mentions the circumstances where the ISP properly responds to a notice from the right owner, and does not address a situation where the ISP, on its own initiative, takes measures to prevent infringement upon its own finding or awareness of the infringing fact. For instance, how does one determine the liability of an ISP that in spite of not having received any notice from the right owner, locates the infringing linked material and on its own initiative, expeditiously removes the links to that material? Obviously, under this circumstance, the ISP should not be liable for its information location service. Likewise, the latter part of this article on the ISP’s joint liability merely regards the actual knowledge or constructive knowledge as a condition for liability, but neglects to consider whether the ISP has properly responded to such knowledge. It is necessary to add another condition for such joint liability wherein the ISP does not expeditiously remove or disable access to the infringing material upon acquiring the actual knowledge of illegal links.

Another issue is related to the requirement of obtaining financial benefits. Unlike Article 22, Article 23 of the RNDI grants the ISP immunity from liability of damage without requirement of ‘never directly receives a financial benefit’. In consequence, even if the ISP has obtained a financial benefit directly arising from the copyright infringement, it can be exempted from liability of damage, on the condition that other necessary conditions for immunity are satisfied. However, it does not exclude the ISP’s liability in case of unjust enrichment. In other words, the ISP has an obligation to return the unjust enrichment acquired from the infringing activity to the right owner under civil law. Different from China’s approach, the DMCA provides that the ISP offering information locating service should ‘not receive a financial benefit directly attributable to the infringing activity’ when seeking safe harbour protection.

It is interesting to see that the e-Commerce Directive does not contain a similar safe harbour provision for information location service. The main reason is that the legislature believes that a search engine would only transmit facts, so that these kinds of ISPs would in principle not be liable for those facts. Nevertheless, this opinion is challenged by the fact that more and more ISPs who offer information locating tools also conduct selection, organization or classification of located information. It is difficult to say that such information location service is automatically completed according to technical arrangements. The EU has however, begun to consider the addition of a new article to deal with this issue.

**Notice-and-takedown Procedure**

The notice-and-takedown procedure is repeatedly stipulated in China’s legislative, judicial and administrative documents. Under the RNDI, if the right owner believes that the material, for which the ISP provides services of storage, search or links, violates its copyright, he may send a written notice to that ISP and require it to remove or disable access to the illegal material (Article 14). Upon receiving this notification, the ISP should promptly remove or disable access to the alleged material (Article 15). The elements of such notification include the name, contact information and address of the right owner, the name and URL address of the alleged material, and initial evidence of infringement (Article 14). The judicial interpretation released by the Supreme People’s Court further clarifies that the ISP would be jointly liable for copyright infringement if it does not, subject to the RNDI, promptly make measures after receipt of the notice.³³ Besides, under the Chinese administrative regulations, the ISP failing to comply with the provisions concerning notice-and-takedown procedure might incur administrative penalties once the administrative authority finds that such failure harms public interests.³⁴

The case of IFPI v Yahoo/Alibaba³⁵ addressed a question whether the notice that does not exhaustively contain the URL address of the alleged material, constitutes an eligible notice of the notice-and-takedown procedure under the Chinese laws. In this case, Alibaba, a famous ISP in China, provided links to infringing resources. Before bringing this action, IFPI sent a notice of a copyright violation to Alibaba, which contained the names of the infringed songs and corresponding singers, as well as one URL address of each song as an example, and required Alibaba to remove all the URL links involving the alleged songs from its website. However, Alibaba failed to expeditiously take measures after receiving this take-down notice. The defendant argued that the notification of the claimed infringement was not detailed enough, because it did not list all the URL links of the infringed
songs. Nevertheless, the court rejected this argument and held that the notification would be fully qualified as long as information offered by such notification is reasonably sufficient to permit the service provider to locate the material, even though it does not list the URL addresses of the alleged material one by one.  

The Directive Opinions of Beijing’s Higher Court adopted a similar approach that ‘if a notice sent to an ISP by the right owner does not include the network address of the alleged infringing works, performances or sound or video recordings, but the information provided in the notice is sufficient for the ISP to accurately locate the alleged infringing works, performances or sound or video recordings, the notice sent by the right owner may be determined to be a warning with evidence’. This indicates that a notification without the URL address of the alleged material may also initiate a notice-and-takedown procedure as long as it provides sufficient information for exact location. The Courts’ opinion that information sufficient to accurately locate the infringing material creates a circumstance to constitute the ISP’s constructive knowledge of red flag is seemingly contradictory to the rules laid down in Article 14 of the RNDI under which the URL address is a prerequisite of a qualifying notification.

Conclusion

The limitation of the ISP’s liability has been an issue of debate in China for long. It is important to strike a balance between the interests of stakeholders by imposing reasonable liability upon the ISP. However, some basic aspects remain unclear in China’s existing legal regime. These defects are caused by ambiguous wording, absence of explicit definition of fundamental concepts, lack of uniform legislative and judicial interpretation, and so on. The legislature should endeavour to reduce the ambiguities existing in the current system in order to provide an effective and efficient copyright protection. Moreover, the practice of other countries in this regime can be reviewed, to determine the feasible practice to be followed in China.

Acknowledgement

The author is thankful to Prof Tobias Cohen Jehoram and Prof Maarten Kroeze for their kind help.

References

4 Interpretation of the Supreme People’s Court on Several Issues Concerning the Application of Law in the Trial of Cases Involving Copyright Disputes over Computer Network, 2006.
7 Ciwen Ltd v Wangtong Hainan Ltd, The Hainan Higher People’s Court No Qiongminzherzhongzi 29/2006.
14 Jacob Assaf and Argento Zoe, To cache or not cache; that is the question-P2P ‘system caching’ –the copyright dilemma, Whittier Law Review, 31 (3) (2010) 421-490.
15 RIAA v Verizon, 351 F. 3d at 1238 (DDC 2003).
17 Io Group Inc v Veoh Networks Inc 568 F. Supp. 2d 1132 (N.D. Cal. 2008).
22 Perfect 10 v CCBill, 488 F. 3d 1102 (9th Cir 2007).
25 *Beijing Xingzhuan Ltd v Shanghai Quan Tudou Ltd*, The Shanghai Higher People’s Court, No Hugaominsanzhizhong 62/2008.


33 Article 4, Interpretation of the Supreme People’s Court on Several Issues Concerning the Application of Law in the Trial of Cases Involving Copyright Disputes over Computer Network, 2006.

34 Article 11, Measures for the Administrative Protection of Internet Copyright, 2005.
