ASPEN PUBLISHERS

The COMPUTER & INTERNET Lawyer

Volume 27 ▲ Number 7 ▲ JULY 2010

Ronald L. Johnston, Arnold & Porter, LLP Editor-in-Chief*

A Comparative Copyright Analysis of ISP Liability in China Versus the United States and Europe

By Seagull Haiyan Song

How to determine the liability of Internet service providers (ISPs)[1] has become one of the most debated issues in Internet law and policy. ISP liability can arise in a number of legal fields, including trademark, trade secrets, unfair competition, defamation, privacy, and of course copyright law. This article will primarily address ISP liability under the copyright law regime in China[2]—under what circumstances should ISPs be held liable when copyrighted material is transmitted, or made available, over the Internet without authorization of copyright holders.[3]

Seagull Haiyan Song is Senior Counsel at the Walt Disney Company and member of the Bar of California and the People's Republic of China Bar Association. This article was prepared for Ms. Song's JSD thesis at U.C. Berkeley (Boalt Hall). Ms. Song is most grateful to her JSD supervisor, Molly Van Houweling, for guiding her during the process and to her former colleagues Michele Woods and Ron Johnston and her current colleagues at Disney for their comments and help on this article.

ISPs might become vulnerable to charges of copyright infringement, whether direct or indirect, during the process of hosting Web pages, forwarding and processing messages, newsgroups and emails, providing online chat venues, and linking users to sites and services in the Internet world.[4] When ISPs directly infringe copyrights of rights holders, such as serving as an Internet content provider (ICP) instead of a mere conduit, copyright holders can certainly bring a direct infringement claim against such ISPs/ICPs. More often, ISPs might be held secondarily liable for copyright infringement attributed to them by the direct infringement activities of its end-users. Given the vast volume of information traveling over the Internet, it would be difficult to expect ISPs to act as the Internet police to enforce IP rights.[5] As such, to strike a balance between protecting rights of copyright holders and shielding ISPs from liability, a number of countries have developed specific ISP legislation and secondary liability theories to restrict ISPs' liabilities from infringement activities conducted by others.

Wolters Kluwer
Law & Business

There have been no universally accepted secondary liability theories worldwide. Nonetheless, an overall review of copyright infringement cases in the United States, Europe, and other jurisdictions shows that courts will generally consider the following factors when determining the liability of ISPs:

- An ISP's knowledge of infringing activities by its end-users;
- Its intent to infringe;
- Material contribution to the infringing activity;
- Ability and rights to control the access or infringing activities; and
- Direct financial benefits arising from infringing activities.

The second part of the article begins with a review of ISP liability theories in the United States and Europe as developed in a number of copyright infringement cases in the last decade, especially after the effective dates of the 1998 Digital Millennium Copyright Act (DMCA)[6] and the 2000 European Union E-commerce Directive. The third part will first discuss the copyright law regime in China, in particular the 2006 Regulation on the Protection of the Right of Communication through Information Networks (the Information Network Regulation), and then examine several ISP liability cases decided by the Chinese courts. The last parts of the article will address problems and uncertainty under the existing PRC copyright law as to the liability of ISPs and then propose a number of recommendations to be considered in future legislative reform.

ISP Liability in the United States and Europe

The United States

ISPs can certainly be held liable for direct infringement if they directly infringe copyrights of rights holders. A typical example would be if an ISP, functioning as an ICP, provides infringing content stored on its own server over the Internet without authorization. Having recognized this possibility, however, this part will focus only on the secondary liability of ISPs, a more controversial issue in Internet law and policy.

Secondary Liability Theories Developed in the United States

The US courts have developed contributory and vicarious liability theories from the common law system when holding ISPs secondarily liable for copyright infringement. To establish a contributory liability claim, a copyright holder must prove (1) that there has been a direct infringement; (2) that the accused contributory infringer has actual or constructive knowledge of the infringing activity; and (3) that the accused contributory infringer caused or materially contributed to the underlying direct infringement.[7]

To prevail on a vicarious liability theory, a copyright holder needs to prove (1) that there has been a direct infringement; (2) that the accused vicarious infringer had the right and ability to control or supervise the underlying direct infringement; and (3) that the accused vicarious infringer derived a direct financial benefit from the underlying direct infringement.[8]

In *MGM v. Grokster*,[9] the US Supreme Court also developed a new secondary liability theory—inducement theory—from patent law.[10] Inducement theory requires both the "affirmative intent"[11] and "active steps"[12] of an ISP in a copyright infringement case to hold it secondarily liable for copyright infringement.

DMCA §512

The Online Copyright Infringement Liability Limitation Act (OCILLA) is a federal law that creates a conditional safe harbor for online service providers (OSPs), including ISPs and other Internet intermediaries, by shielding them from liability for the infringing acts of others. OCILLA was passed as a part of the DMCA and is sometimes referred to as the safe harbor provision or as DMCA §512.

DMCA §512 provides that an ISP might be exempt from liability for copyright infringement stemming from transmitting,[13] caching,[14] hosting,[15] or linking[16] to infringing materials. To trigger the safe harbor provisions, an ISP must satisfy two threshold requirements. First, the ISP must "adopt and reasonably implement a policy"[17] of addressing and terminating accounts of users who are "repeat infringers."[18] Second, the ISP must accommodate and not interfere with "standard technical measures."[19]

Section 512(c) is the most commonly quoted provision in recent ISP liability cases because it might immunize Web sites that inadvertently *host* infringing content uploaded by users. In addition to the two general threshold requirements with which ISPs must comply, §512(c) also requires that the ISP:

1. Not have actual knowledge or be aware of facts or circumstances from which infringing activity is apparent;
2. 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, and

3. Upon obtaining such knowledge or awareness or receiving notice from copyright owners or their agents, acts expeditiously to remove or disable access to the purported infringing material.[20]

Relationship Between Secondary Liability Standards and §512

Because of the similar language in DMCA §512(c) and the elements in contributory and vicarious liability theories in respect of "knowledge," "direct financial benefits," and "right and ability to control," there has been a debate as to whether the same standards for secondary liability apply in DMCA §512(c).[21] Unfortunately, the existing case law fails to provide clear guidance in this respect.

Contributory Liability: Knowledge of Infringing Material

Under contributory liability, a defendant can be held liable if he knows or has reason to know of another's direct infringement and has materially contributed to it.[22] Under the DMCA §512(c), however, mere knowledge of another's direct infringement and material distribution are not dispositive. An OSP can still claim safe harbor protection if it "acts expeditiously to remove or disable access to the [infringing] material" upon obtaining such knowledge or awareness.[23] There are two ways that an OSP might have actual knowledge or awareness of infringing materials and activity: (1) take-down notice from the copyright owner and (2) the existence of red flags.

The first way that an OSP can have actual knowledge of infringing material and activity is through the copyright holder's written notification of claimed infringement to the OSP's designated agent. If the notice substantially complies with six requirements[24] set out in DMCA §512(c)(3)(a), the OSP must expeditiously remove or disable access to the allegedly infringing material.[25]

Unfortunately, it is unclear from the existing case law how perfect a take-down notice should be. Although the statute reads that compliance with notice requirements must be only "substantial," in *Perfect 10 v. CCBill*,[26] the court emphasized that the language of the statute requires "substantial compliance with *all* of 512(c)(3)'s clauses."[27] To pose an even stricter requirement on the notice, the *CCBill* court held that a properly constructed notice must exist within the bounds of a single correspondence.[28] The *CCBill* court reasoned that to allow a copyright owner to "cobble together adequate notice from separately defective notices" would pose an undue burden on the ISP that would then have to track all incoming correspondence to identify all the elements required by §512(c)(3).[29] As such, even if CCBill had received several notices regarding potential copyright infringement, the court concluded that defective notice could not be read to give CCBill the knowledge required by DMCA §512(c)(1)(a).[30] Similarly in *Hendrickson v. eBay,*[31] the plaintiff sent eBay a general cease-and-desist letter but "did not explain which copies of 'Manson'…were infringing copies [and did not] fully describe [Hendrickson's] copyright interest,"[32] thus the court considered the copyright holder's failure to satisfy the requirements of a proper notification by identifying infringing material as insufficient to trigger an ISP's duty to act.[33]

In *ALS Scan, Inc. v. RemarQ Communities, Inc.*,[34] however, the Fourth Circuit took a less stringent view of a copyright owner's compliance with the DMCA §512(c) notification requirement. In this case, ALS Scan sued the defendant for knowingly allowing its user to post and access newsgroup listings that contained infringing copies of the plaintiff's copyrighted photos. ALS Scan's notice directed RemarQ to two newsgroups containing infringing copies of its images but did not specify the "identity of the pictures forming the basis of the copyright claim."[35] Nonetheless, the court found ALS Scan's notice acceptable, reasoning that the safe harbor immunities are "not presumptive, but granted only to 'innocent' service providers who can prove that they do not have actual or constructive notice."[36] In holding that copyright owners need not specify infringing content with specificity, the court posed a bigger burden on ISPs to enforce.

The second way that an OSP can be put on notice is referred to as the red flag test.[37] The red flag test stems from the language in the statute that requires an OSP not be "aware of facts or circumstances from which infringing activity is apparent."[38] This test contains both a subjective and objective element. Objectively, the OSP must know that the infringing material resides on its system. Subjectively, the reasonable person standard applies when the "infringing activity would have been apparent to a reasonable person operating under the same or similar circumstances."[39]

In practice, the identification and application of the red flag is not clear either. In *Perfect 10 v. CCBill*, the court rejected the plaintiff's argument that red flags existed because of two domain names, *illegal.net* and *stolencelebritypics.com,* to which the defendant had provided services. Rather, the court found that the domain names did not establish copyright infringement in themselves because the words "illegal" and

"stolen" could "be an attempt to increase their salacious appeal, rather than an admission that the photographs are actually illegal or stolen."[40] In *In re Aimster*,[41] however, the court deemed that an ISP's willful blindness to infringing activities amounted to constructive knowledge.[42]

Vicarious Liability: Financial Benefit and Right and Ability to Control

Under vicarious liability, a defendant can be held liable if he has "a direct financial interest in such activities" and "right and ability to control." There has been a debate, however, as to whether the same standard of vicarious liability should apply in DMCA §512 (c)(1)(B). We have seen various opinions from courts in this respect.

It is unclear from the existing case law how perfect a take-down notice should be.

To start with the direct-financial-benefit prong, there are a number of conflicting opinions interpreting the relationship between common law vicarious liability standards and DMCA provisions. For instance, in *CCBill*, the Ninth Circuit expressly recognized that the elements in DMCA §512(c)(1)(B) must be interpreted based upon their meaning at common law by stating that "'direct financial benefit' should be interpreted consistent with the similarly-worded common law standard for vicarious copyright liability."[43] Similarly, in *A&M Records v. Napster*,[44] the court held that copyrighted material on Napster's system created a "draw" for customers that resulted in a direct financial benefit because Napster's future revenue was directly tied with the increase in user base.[45] Here, the judge in both cases adopted the exact same standard of vicarious liability when interpreting DMCA §512 (c).

There are also cases, however, in which the courts applied a stricter standard of financial benefit to the DMCA requiring a higher level of proof for establishing direct financial benefit. For instance, in *CCBill*, the court quoted the legislative language[46] and 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.'"[47] Similarly, in *Ellison v. Robertson*,[48] involving the unauthorized posting of Harlan Ellison's works by a third party on a USERNET newsgroup accessible by AOL users, the court also applied a stricter interpretation of "direct financial benefit" and tightened the requirements of proof. The court held that the plaintiff had failed to support the vicarious liability claim because he had not shown a casual connection "between AOL's profits from subscriptions and the infringing activity taking place on its USENET servers."[49] The court found no evidence that "AOL attracted or retained subscriptions because of infringement."[50]

With regard to the element of "right and ability to control," there are also conflicting opinions as to what standards should apply. In *Napster*, the court believed that Napster had the ability to control the infringing activity because it could block the user's access to its systems.[51] In *Hendrickson v. eBay, Inc.*,[52] however, the court adopted a much narrower standard of the DMCA compared with the common law vicarious liability standard. The district court explained that the "right and ability to control" the infringing activity cannot simply mean the ability of a service provider to remove or block access to materials posed on its Web site or stored on its system. The court reasoned that the DMCA specifically requires an OSP to remove or block infringing materials upon notification and to adopt and reasonably implement a policy against repeated infringers; therefore, the Congress could not have intended for courts to find that an OSP has lost immunity because it engaged in acts that are specifically required by the DMCA.[53]

ISP Cases in the United States

The following paragraphs provide a quick overview of a few major court opinions that applied indirect liability theories to ISPs in recent years, including contributory, vicarious, and inducement infringement theories. All these cases touched the unsettled questions discussed already.

The Napster *Case*

In the *Napster* case,[54] the plaintiff music industry admitted that Napster did not directly make or distribute any of their copyrighted works. Rather, the plaintiff argued for contributory and vicarious infringement liability theories and requested a preliminary injunction against Napster. The injunction was appealed and affirmed by the Ninth Circuit in February 2001.[55]

When examining the claim of contributory infringement, the Ninth Circuit upheld the lower court's decision and held that Napster had actual knowledge of the infringing activity evidenced by its internal company emails and the list of 12,000 infringing files provided by the Recording Industry Association of America. The court also ruled that Napster had materially contributed to the infringing activity because it provided sites and facilities to its infringing end-users.[56]

Therefore, Napster was found liable for contributory infringement.

With regard to the vicarious liability theory, the Ninth Circuit supported the lower court's finding and believed that Napster had the ability to control the infringing activity because it could "block" the user's access to its systems.[57] The court also found that Napster had derived direct financial benefits from the infringing activities of its end-users because this activity "acted as a 'draw' for customers,"[58] when Napster's revenue was directly tied to the number of times that advertisements were viewed on the system.

The Ninth Circuit did not discuss in detail whether the defense asserted by Napster in citing DMCA §512(d) should apply, but recognized that this issue would be fully developed at trial.

The Aimster *Case*

In the *Aimster* case,[59] the music industry made the same contributory infringement and vicarious liability arguments as it did in *Napster*. The music industry successfully obtained an injunction that eventually shut Aimster down while the case was pending on the merits.

The Seventh Circuit addressed the contributory infringement claim[60] but did not fully accept the vicarious liability argument. When addressing the actual knowledge of Aimster regarding infringing materials, the court focused on the "tutorials"[61] that specifically encouraged Aimster users to download popular copyrighted music and held that the actions of Aimster had amounted to "willful blindness,"[62] which constituted "knowledge in copyright law,"[63] and thus found Aimster liable for contributory infringement.

When responding to Aimster's defense citing DMCA §512, the court ruled that the DMCA safe harbor provision should not apply to Aimster because Aimster did not even meet the threshold requirement of "reasonably [implementing a policy] to prevent the user of its services by repeat infringers."[64] Rather, Aimster invited repeated infringers, showed them, and even taught them how to violate plaintiff's copyrights.[65] Therefore, the court rejected Aimster's defense for safe harbor protection.

The Grokster *Case*

In *MGM v. Grokster*,[66] although the entertainment industry originally argued both the contributory infringement and vicarious liability theories, the Supreme Court did not adopt either of these claims but proposed a new theory of copyright "inducement liability" based on patent law:[67] "[O]ne who distributes a device with the object of promoting its use to infringe copyright, as shown by clear expression or other affirmative steps taken to foster infringement, is liable for the resulting acts of infringement by third parties."[68]

According to the Supreme Court, the inducement theory requires both "affirmative intent"[69] and "active steps"[70] by the defendant. The Supreme Court pointed to a number of things that constituted "active steps" for inducement purposes: advertisements attracting Grokster users to use its servers,[71] newsletters with links to articles that discussed infringing uses of the software,[72] and customer support that assisted users who had trouble downloading infringing materials.[73] With reference to the issue of "intent," the Court ruled that there was sufficient evidence, such as internal communication and advertising, of efforts to attract Napster users, and failure to implement filtering or other technology to block infringing activity, to show that Grokster had an affirmative intent to infringe.

IO Group Inc. v. Veoh Networks, Inc.

In *IO Group Inc. v. Veoh Networks Inc.*,[74] IO Group alleged that Veoh, a flash video Web site operator that provides the ability to upload and share user-provided video content over the Internet, was responsible for copyright infringement by allowing its users to upload and view IO Group's copyrighted films and clips without authorization. IO Group requested summary judgment based on direct, contributory, and vicarious copyright liability claims.

The court first dismissed IO Group's direct infringement claim by holding 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... But Veoh does *not* itself *actively participate or supervise* the uploading of files. Nor does it *preview or select* the files before the upload is completed. Instead, video files are uploaded through an *automated* process which is initiated entirely at the volition of Veoh's users.[75]

Then the court went on to address the indirect liability of Veoh. Instead of responding to the plaintiff's contributory and vicarious liability claims, the court addressed only whether Veoh should qualify for the DMCA §512(c) safe harbor provision. In particular, the court inquired whether:

1. The infringement activity was conducted at the direction of a user;

2. Veoh has actual or constructive knowledge of infringing activity;

3. The expeditiousness of Veoh's acts to remove or disable access to material; and

4. Veoh has the right and ability to control infringing activity, or if it does, whether it has received a financial benefit directly attributable to the infringing activity.

The court first found that the infringing activity was *initiated entirely by its users*, and Veoh neither actively participated in nor supervised the uploading of files.[76] Turning to *actual* and *constructive knowledge* of infringing activities, the court found that, because plaintiff never sent a take-down notice to Veoh prior to filing the law suit, Veoh did not have actual knowledge of infringing activity.[77] Also, citing *Corbis Corp. v. Amazon.com, Inc.,*[78] the court believed that the red flag test should be interpreted as "whether the service provider *deliberately* proceeded in the face of *blatant* factors of which it was aware,"[79] and held that no evidence showed that Veoh had constructive knowledge of infringing activity. With reference to the issue of *expeditious acts to remove or disable access*, the court noted that, although Veoh never received the take-down notice from plaintiff, it voluntarily removed all adult content from its Web site. Further, the court seemed to be impressed with Veoh's swift routine response to take-down notices, in which Veoh "responds and removes noticed content as necessary *on the same day* the notice is received."[80] Last, regarding the issue of *right and ability to control*, the court differentiated an ISP's right and ability to control "its system" from the right to control "the infringing activity" and held that Veoh did not have the right and ability to control infringing activity.[81] In the end, the court concluded that Veoh was entitled to DMCA §512 safe harbor protection, thus granting Veoh's motion for summary judgment.

Other Cases

There are some other ISP liability cases currently pending in the US courts. For instance, in *Viacom Intern. Inc. v. YouTube Inc.*,[82] Viacom brought a suit against Google and YouTube, the most popular video-sharing Web sites, for direct copyright infringement as well as contributory and vicarious infringements on March 13, 2007, seeking $1 billion in damages.[83] YouTube users can post videos and recommend and share videos with YouTube visitors and employ YouTube's sophisticated searching and indexing features to locate and watch other user-generated videos. The litigation is currently in the discovery phase.

Europe

The European Union E-commerce Directive

The European Union E-commerce Directive[84] adopts the definition of "Information Society Service"[85] under Article 1.2 of Directive 98/34/EC to refer to ISPs and addresses the civil and criminal liabilities of ISPs acting as intermediaries.[86] The Directive provides that ISPs will not be held liable in any field of law in which an application of strict liability would impair the expansion of electronic commerce within the EU. The approach is called "horizontal" because it addresses liability regardless of the grounds for liability; it therefore applies not only to copyright law but also to other areas of law such as defamation and obscenity.[87]

Among the ISP liability cases decided in European countries, the safe harbor provision for "hosting services" under Article 14 seems to be the most commonly encountered issue.

Although a number of secondary liability cases have been decided under the specific provisions of Article 12-14 of the Directive, there seem to be no clearly labeled secondary liability theories to ISPs under the EU case law. Based on the Directive, an ISP is exempt from liability when it serves as a "mere conduit" (Article 12) or provides "temporary caching" (Article 13) for the sole purpose of making the transmission of content more efficient, is of a mere technical, automatic, and passive nature, and when the ISP has neither knowledge of nor control over the content being transmitted or stored.[88] ISPs that provide content storage, *i.e.*, "hosting services" (Article 14), are exempt from liability provided that they do not have "actual knowledge or awareness of facts or circumstances" of illegal activities and "expeditiously remove or disable" access to content upon receipt of such knowledge or awareness.[89] Although Article 15 of the Directive prevents member states from imposing a "general duty to monitor," it does not prevent courts or administrative authorities of member states from imposing a monitoring obligation in a specific, defined individual case.[90]

Recent ISP Liability Cases in Europe

Among the ISP liability cases decided in European countries, the safe harbor provision for "hosting services" under Article 14 seems to be the most commonly encountered issue argued before the courts. Courts generally need to decide whether the accused ISP qualifies

as a hosting service and, if it does, whether it should be exempt from liability for copyright infringement.

MySpace *(June 2007, France)*

In June 2007, a French humorist Jean-Yves L., also known by the name of *Lafesse* (literally "the buttock"), successfully sued MySpace for infringement of the author's rights after several of his skits were posted by users on the Web site.[91] The French High Court of First Instance rejected the defendant's argument that it was providing a "hosting service" qualifying for safe harbor protection under Article 14. Rather, the court held that MySpace should be categorized as a "publisher"[92] because it allowed members to create personal Web pages within a specified frame structure, including video uploading and broadcasts, and also generated revenue from its advertisements. As a result, the court ruled that immunity under Article 14 of the E-commerce Directive should not apply to MySpace, and MySpace was found directly liable for copyright infringement.[93]

DailyMotion *(2007, France)*

In *DailyMotion*, the plaintiff, producer/director/distributor of the film "Joyeux Noel," sued the UGC Web site DailyMotion for hosting unlawful copies of the film.[94] The court qualified DailyMotion as a hosting provider but nonetheless found the defendant liable for copyright infringement on the grounds that DailyMotion had *actual knowledge* of the presence of illegal content on its Web site, its architecture and technical means enabled illicit activities, and its very success depended on the making available of copyrighted materials by its users.[95] Therefore, the safe harbor protection in Article 14 did not apply to DailyMotion.[96] When DailyMotion recalled the proscription of a general obligation to monitor as imposed by Article 6-I-7 LCEN[97] (implementation of Article 15 E-commerce Directive), the court rejected its argument and held that the prohibition applies only in cases in which the unlawful activities were not generated or induced by the intermediary itself.[98] For intermediaries that provide users with means for infringing copyright, they have a duty to carry out prior control for the prevention of such user behavior.[99] DailyMotion subsequently announced that it would install fingerprint filtering technology after the case.[100]

What is noteworthy is that, although the E-commerce Directive sets out a basic requirement for EU member states to enforce IP rights, each individual jurisdiction still has discretion in interpreting the Directive. The following *Google (2007), eBay* (2008), and *SARBAM* (2007) cases, which were decided by French and Belgian courts respectively, are good examples of such various interpretations.

Lancôme v. eBay

In *Lancôme v. eBay*,[101] Lancôme claimed that a huge percentage of the cosmetic products bearing its trademark made available on the auction Web site (eBay) were counterfeits[102] and requested that eBay take necessary measures to counteract the infringement activities. Due to eBay's lack of action in this respect, Lancôme sued eBay in Belgium for not doing enough to prevent trademark infringement. EBay argued that it is only a hosting service provider and has no general duty to monitor. The Belgian Commercial Court accepted eBay's argument and held that, as an online auctioneer, eBay had no general duty to monitor what users published in the service. The court also found that eBay had *no actual knowledge* of infringing activity, it had *removed* infringing products immediately after receipt of the take-down notice, and it did not have "editorial control" over what users would publish.[103] As a result, the court dismissed Lancôme's claims and found eBay not liable.[104]

Google

In *SARL Zadig Productions, Jean-Robert Viallet et Mathieu Verboud v. Ste Google Inc. et AFA,*[105] however, the French court imposed a much higher standard of care on ISPs to enforce IP rights. In *Google*, the plaintiff Zadig Productions, a French film company, sued Google for hosting its movie "Tranquility Bay" on its Web site without authorization. Although Google had removed the unauthorized content from its Web site each time that it received a take-down notice, the film was repeatedly reposted on the Web site by its users. The court agreed that Google qualified as a "hosting service" defined under Article 14 of E-commerce Directive.[106] The court found Google secondarily liable for copyright infringement, however, because "it had not done enough" to enforce IP rights.[107] The court believed that, after Google was informed of the existence of infringing copies of the film, it was under an obligation to implement any means necessary to avoid future dissemination. The fact that Google had failed to comply with the conditions of Article 6-I-2 LCEN in respect to every subsequent uploading led the court to conclude that it was liable for copyright infringement.

SABAM v. Scarlet

In *SABAM v. Scarlet*, the plaintiff, the Belgian Society of Authors, Composers and Publishers (SABAM), sued the Belgian Web site Scarlet for knowingly permitting the illegal downloading of SABAM's protected works through the P2P file sharing on its Web site.[108]

The Brussels Court of First Instance ordered Scarlet to take more proactive measures to stop the unauthorized exchange of protected materials by its subscribers and to install the content management and identification fingerprint-based system.

Similar ISP liability cases could also be found in Germany[109] and Sweden (*Pirate Bay*, 2009),[110] where the courts recognized the "hosting" status of ISPs but nonetheless found the ISPs liable for copyright infringement because they had failed to satisfy the safe harbor provision of Article 14 of the Directive.

ISP Legislation and Cases in China

Chinese ISP Legislation

The existing Chinese copyright law provides certain protection to copyright owners in the digital world. For instance, the People's Republic of China (PRC) Copyright Law and its Implementing Regulations, adopted in 1990 and revised in 2001, set out basic copyright protection for both copyright owners and neighboring rights owners.[111] China also adopted the Regulations for the Protection of Rights of Communication through Information Networks (2006 Regulations) to address increasing concerns over online piracy.[112] The 2006 Regulations follow a number of principles set out in the DMCA, including the safe harbor provisions for ISPs.

Although China does not have specific secondary liability theories, ... Chinese courts considering ISP liability look to factors similar to those assessed by US courts.

Article 20 of the 2006 Regulations protects an ISP that merely provides automatic access service at the direction of its subscribers (mere conduit) from liability if it does not select or alter the transmitted works or makes the transmitted works available only to the targeted recipients rather than to the general public. Article 21 immunizes an ISP that provides automatic storage services (automatic caching) from liability if it does not alter the transmitted works and does not affect the access of the original content provider. Article 22 states that an ISP that provides network storage services (hosting services) for subscribers will not be liable if it does not alter the transmitted works, does *not know* or has *no reasonable grounds to know* that the transmitted materials are infringing, and has not derived direct benefits from the transmission. In addition, to be immune from liability, an ISP providing hosting services must immediately remove infringing materials after it receives take-down notices from proprietors. Article 23 protects an ISP that provides searching/linking services from liability if it immediately removes or disables the access to infringing materials upon receipt of a take-down notice from proprietors and does *not know* or *should not know* that the linked content is infringing.

The legal basis to hold an ISP liable for the direct infringement of its end-users in China lies in its Civil Code[113] and the recently enacted PRC Tort Law[114] and its joint-liability theory. The Supreme Court Interpretations and Opinions, which are legally binding in China, also discuss the joint-liability theory. Article 4 of the Interpretations of the Supreme People's Court of Several Issues Regarding Applicable Laws for the Hearing of Copyright Disputes Involving Computer Networks issued in 2000 provides that an ISP will be jointly liable with other infringing parties provided that:

> a) an ISP infringes via the Internet a copyright held by another party; or causes or assists a third party to do so; or b) is aware of user infringement of a copyright held by another party or has been properly warned of such infringement by the copyright owner, but fails to remove the relevant content.[115]

Although China does not have specific secondary liability theories, including contributory, vicarious, or inducement theories developed in the United States, Chinese courts considering ISP liability look to factors similar to those assessed by US courts, including an ISP's knowledge of infringement,[116] intent, ability and rights to control infringing activity, financial benefits arising from infringing activities, and contribution to the infringing activity, for example.

ISP Liability Cases in China

Based on the statistics provided by the Beijing High Court, copyright infringement cases occupied a major share of all IP-related cases filed before Chinese courts in recent years, when the copyright-related cases rose from 40 percent in 2007 to 47 percent during the first half of 2009.[117] Among all the copyright infringement cases involving liability of ISPs, Article 22 (hosting) and Article 23 (searching/linking) are the most frequently encountered provisions.

ISP Direct Liability

In *Columbia Pictures v. Sohu.com*,[118] Columbia Pictures filed a lawsuit against Sohu for copyright infringement after discovering that Sohu had provided subscription-based access to an unauthorized online video archive of approximately 100 US films. The archive included

films produced by Columbia Pictures and other studios. Columbia Pictures sought damages of RMB 1 million (around US$50,000) for economic losses and costs of RMB 201,000 (around US$35,000).[119]

The Beijing First Intermediate Court ruled that Sohu.com had infringed Columbia Pictures' "rights of communication through information networks" and ordered Sohu to cease the infringement, publish an apology on its Entertainment home pages for three consecutive days, and pay a damage of RMB 191,000 (around US$23,000).[120]

ISP Indirect Liability

ISPs Providing "Hosting" Services (Article 22)

In *Success Media v. Alibaba*,[121] the plaintiff sued Alibaba for copyright infringement when Alibaba was alleged to have enabled the uploading and sharing of the TV episodes "Struggle" (1-15), for which the plaintiff enjoyed exclusive broadcasting rights in China, at the user-generated-content section of its site (*www.cn.yahoo.com*) without authorization.

Alibaba argued that the Article 22 (hosting service) safe harbor provision should apply because, as an ISP providing automatic storage/hosting services, it did not alter the transmitted works uploaded by its users, had no actual knowledge or reasons to know that the transmitted materials were infringing, and had not derived direct benefits from the transmission.[122] Alibaba further argued that it also immediately removed the infringing material after it received the take-down notice from the plaintiff and thus should not be held liable for copyright infringement.[123]

The Beijing Chaoyang District Court accepted Alibaba's arguments and held Alibaba not liable for copyright infringement.[124] This decision was later overruled by Beijing No. 2 Intermediate Court, which qualified Alibaba as a hosting service provider but nonetheless found it jointly liable for copyright infringement on the ground that Alibaba *knew or should have known* that the uploaded content was infringing.[125]

When addressing the knowledge element of the defendant, the court reasoned that the TV episodes were uploaded during the same period as the prime time of local TV broadcast.[126] Moreover, Alibaba had provided a detailed introduction of the TV series, including posters, actors/directors, and synopsis, for example, on its home page.[127] Therefore, the defendant knew or had reasonable grounds to know that the uploaded TV episodes were provided by its users without authorization. As such, the Article 22 safe harbor provision did apply, and Alibaba was held liable for copyright infringement.[128]

ISPs Providing "Searching/Linking" Services (Article 23)

In *IFPI v. Baidu,*[129] IFPI sued Baidu, one of the largest Internet portal sites in China, for direct copyright infringement. Baidu argued that it was providing only a "searching/linking service" to its users and did not directly infringe the rights of copyright holders.[130] The Beijing No. 1 Intermediate Court agreed with Baidu's arguments, acknowledged Baidu's status as a linking service provider, and ruled that Article 23 safe harbor provision should apply.[131]

When addressing the take-down provision under Article 23, the court dismissed IFPI's warning letter as a "defective notice" and held that, since IFPI had failed to send a qualified take-down notice, Baidu was not put on notice of the infringing activity, thus should not be liable for copyright infringement.[132] The Beijing High Court later affirmed the Intermediate Court's decision.[133]

In a similar copyright infringement case brought six months later by the same plaintiff against a similar defendant,[134] however, the search engine *Alibaba/cn.yahoo.com*, the same Beijing High Court came to an entirely different conclusion and found the defendant jointly liable for copyright infringement.

Similar to Baidu, users were downloading music via Web links that appeared in search engine results. Unlike *IFPI v. Baidu,* however, in which the plaintiff never explicitly brought the indirect liability claim, IFPI sued the defendant on both direct and indirect liability claims in this case. As with *IFPI v. Baidu*, the Beijing High Court dismissed the plaintiff's direct liability claim on the grounds that Alibaba was providing only "searching/linking services" and was not directly liable for copyright infringement.[135]

When addressing the indirect liability claim, the court cited Article 23 and held that Alibaba *should know or should have known* that the search results contained infringing materials based on the repeated take-down notices sent from plaintiff.[136] The court further reasoned that since Alibaba had failed to take sufficient measures to disable/remove access to the infringing content—Alibaba deleted only the specific URL links stated in the notice but failed to delete other search links leading to the same songs identified in the notice—Alibaba was "grossly negligent" in protecting copyrights of rights holder[137] and thus was jointly liable for copyright infringement.

Uncertainty Regarding ISP Liability Under the Existing PRC Copyright Law

Despite the enactment and implementation of the 2006 Regulations and numerous rulings related to ISP liability cases, there are a number of issues that remain unaddressed and need further clarification in future

legislation reform. Because China is not a case-law jurisdiction and precedents decided by courts will not necessarily bind future courts' opinions, we have seen conflicting opinions from various courts with respect to the interpretations of safe harbor provisions from Article 20-23 under the 2006 Regulations. Moreover, since the 2006 Regulations were drafted to address only the video-on-demand (VOD) services[138] and do not cover real-time retransmission of copyrighted works over the Internet, there seems to be a lack of legal basis to prevent unauthorized real-time streaming of programming transmitted over the Internet.

How Perfect Does a Take-Down Notice Need to Be?

There are conflicting views as to how perfect a take-down notice should be. In *IFPI v. Baidu*, the Beijing First Intermediate Court found that, although IFPI sent a general cease-and-desist letter to Baidu, the warning letter did not contain sufficient information, such as particulars of the proprietor and the infringing URL links, and so should not be considered a qualified take-down notice.[139] The court ruled that the plaintiff did not perform his duty to notify, thus the defendant was not put on notice and should not be liable for copyright infringement.[140]

In *IFPI v. Alibaba*, however, the Beijing Second Intermediate Court reached a different conclusion by reasoning that, although the take-down notice sent by IFPI included only a few sample URL addresses directed to the infringing songs rather than an exhaustive list,[141] the take-down notice contained sufficient information to put the defendant on notice. Therefore, the court considered Alibaba's failure to disable all infringing links to be "gross negligence" and thus found the defendant liable for infringement.

Knowledge of an ISP

As with the US law, where knowledge of an ISP is a required element for contributory infringement analysis and safe harbor protection, the 2006 Regulations consider knowledge a factor when analyzing the liability issue. For instance, to be immune from liability, an ISP providing hosting services must "not know or have no reasonable grounds to know that the works, performance, sound recordings…provided by its subscribers infringe other parties' rights."[142] Similarly, an ISP providing linking/searching services cannot claim safe harbor protection if "it knows or should know that the linked works, performances, sound recordings… infringe another party's rights."[143]

Nonetheless, it is still unclear how the Chinese version of the red flag test—that is, knows, has reasonable grounds to know, and should know—should be interpreted and implemented in practice. For instance, one reason that Baidu was deemed not liable for copyright infringement in *IFPI v. Baidu* was that the court believed that the take-down notice prepared by IFPI, which did not include the copyright certificates or exact links directing to infringing Web sites, was not detailed enough. Yet in a later case, *IFPI v. Alibaba/Yahoo*, the court took a more liberal view of the red flag test and ruled that the defendant was put on notice although the list of URL links was not exhaustive.[144]

Similarly, in *Zhongkai Culture v. Shulian Software*,[145] the Shanghai High Court ruled that, because the premier show of the movie was scheduled in November 2005, it should be "apparent" to the defendant Guangzhou Shulian that the uploading of the movie on November 19, 2005, by its end-users was unauthorized.[146] Also taking into consideration other factors, including that the defendant induced and actively facilitated the downloading of POCO software (a P2P software) and uploading of movies, the court found the defendant jointly liable for copyright infringement.[147] The court also took a more liberal view of the red flag test—that is, that the infringing activity should have been apparent to any reasonable person under the same or similar circumstances.[148]

Although none of the aforesaid cases provide clear guidance on how to prove subjective awareness of factors making infringement apparent, it appears that some of the Chinese courts are starting to impose a much higher duty of care for certain types of ISPs before they can claim safe harbor protection. In *Zhongkai Culture v. Shulian Software,* the Shanghai High Court specifically noted that "the duty of care that is imposed on an OSP should be equivalent to the infringement risks that its business models carry."[149] The court pointed out that, since the defendant set up a video-sharing section on its Web site and further provided P2P software to facilitate the downloading of content by its users, it "should know or have reason to know the infringement risks related to its business model."[150] Therefore, the defendant should be charged with a higher duty of care when policing infringing activity.

Ambiguity of "Expeditiousness" in Take-Down Provision

In *IFPI v. Alibaba*, although the defendant Alibaba eventually disabled links to infringing materials one month after the receipt of the take-down notices, the court ruled that Alibaba's failure to *immediately* remove the infringing material and disable the links amounted to "gross negligence" and thus found Alibaba liable for copyright infringement.[151]

In *Liu Jingsheng v. Sohu Aite Technology Ltd.*,[152] a writer and translator sued a search engine for both direct and indirect infringement. The defendant Sohu Aite was alleged to have provided the plaintiff's translated novels on its Web site without authorization. Regarding the direct liability claim, the court found that Sohu Aite was providing only "searching/linking services" as a search engine and so was not liable for direct infringement.[153] When addressing the indirect liability claim, however, the court ruled that the defendant's failure to remove the infringing materials *immediately* after the receipt of the take-down notice, which it waited *seven* days to delete, caused the continuance of infringing activity. Thus Sohu Aite should be found liable for copyright infringement.[154]

It is unclear from the current legislation and case law exactly what constitutes "expeditiousness" of a take-down. Most content owners argue that, given the widespread effect of the Internet, where millions of views and downloads may take place within 24 hours after copyrighted content such as a newly released movie is posted online, the "expeditiousness" of the takedown should be defined as within 24-48 hours after receipt of a take-down notice.[155]

Real-Time Online Piracy

One of the deficiencies under the existing copyright law, especially with the 2006 Regulations, is that real-time online piracy is not appropriately addressed. Article 26 of the 2006 Regulations defines "right of communication through information network" as "rights of communicating a work, performance, sound recording or video recording to the public, by wire or wireless means, where members of the public may access these works *from a place and at a time individually chosen by them*."[156] In other words, the 2006 Regulations are drafted to deal with video-on-demand (VOD) services and do not cover real-time unauthorized retransmission of programming over the Internet.

With regard to this legislation gap, Chinese legislators seem to believe that, since China is a member of the World Copyright Treaty (WCT), which has a broader definition of rights of communication,[157] the WCT definition could be considered a legal basis for enforcing online piracy of real-time streaming over the Internet.

Nonetheless, the self-execution of a WCT provision does not seem to sufficiently solve the problem of real-time online piracy with its current take-down notice requirement under the 2006 Regulations. Because it usually takes hours, if not days, for an ISP to respond to a take-down notice and remove the infringing materials, it will be too late to effectively stop real-time online piracy under the current legal regime.

Recommendations

Among the various legislative proposals that try to clarify the ambiguities under the existing legal regime to better combat online piracy, two recommendations are worthy of specific attention: fingerprint filtering technology and the Graduated Response (GR) program. The fingerprint filtering technology was advocated under the Principles for User Generated Content Services (UGC Principles)[158] signed between user-generated content (UGC) sites and content owners in 2007. The GR program, on the other hand, is more focused on copyright violations using P2P file sharing services.

Fingerprint Filtering: Shared Burden Between ISPs and Copyright Owners

When discussing the application of tort law principles to indirect copyright infringement cases, Peter Menell and David Nimmer described the traditional tort law as "the default framework for balancing conflicting social interactions."[159] Having categorized various indirect copyright liability theories as two indirect tort liability theories—joint liability and agency/enterprise liability[160]—the authors propose to place the responsibility of enforcement on the enterprise or person who profits from the infringing activity and who is better able to control the infringing activity as opposed to the innocent injured plaintiff or the direct infringer whose act caused the loss.[161] This framework is based on the least-cost avoider, efficient risk bearing, and optimal deterrence theories that have been developed through the case law of tort principles.[162] In particular, Menell and Nimmer have urged the courts to consider the "reasonable alternative design" argument when evaluating the indirect liability of the defendant in a copyright infringement case: Should there be a reasonable alternative design that could have afforded much of the utility of the product/service with substantially lower risk of infringement, then the defendant should adopt this alternative design to avoid liability.[163]

The current business model of most UGC sites in China is to derive revenue primarily from the number of times that an advertisement is viewed on its system. By allowing the existence of unauthorized copyrighted content on its site, a UGC site will naturally attract more views, thus receiving more profits from the infringing activities.[164] Based on this business model, it is fair to ask Chinese UGC sites to share the enforcement burden with copyright owners to police copyrights, in particular to request UGC sites to adopt the

reasonable alternative design, that is, a pre-upload fingerprint filtering technology, to prevent unauthorized uploading of infringing content on their sites.

In October 2007, several UGC sites, including MySpace, Veoh, DailyMotion, and Soapbox (via Microsoft), in cooperation with major content owners including Disney, CBS, NBC Universal, and Viacom, signed a set of non-binding collaborative UGC Principles[165] regarding the use of content identification and fingerprint filtering technologies.

The proposed fingerprint filtering technology under UGC Principles would allow the ISP to compare uploaded materials against samples of copyrighted materials (reference material) provided by copyright owners.[166] If uploaded material matches any reference material and falls into the specifications pre-designed by content owners,[167] the uploaded material will be blocked before it is uploaded unless it is licensed from the copyright owners, as identified in the "white list."[168] The initiative seeks to have content owners and UGC sites cooperate in implementing filtering technology in a manner that "effectively balances legitimate interests in (1) blocking infringing user-uploaded content; (2) allowing wholly original and authorized uploads; and (3) accommodating fair use."[169]

Critics of fingerprint filtering technology, ...are concerned that computer and technology might not fully accommodate fair use.

To date, a number of fingerprint filtering technology sites, including YouTube's own developed filtering technology,[170] Audible Magic,[171] Vobile,[172] and Enswer,[173] have been developed and adopted on UGC sites to prevent unauthorized uploading of copyrighted material. A few Chinese UGC sites were also reported to have been developing their own fingerprint filtering technology.[174]

Critics of fingerprint filtering technology, on the other hand, are concerned that computer and technology might not fully accommodate fair use. Michael Sawyer argued in his paper "Fair Use and Feedback: User-Generated Content Principles and the DMCA" that computers might excel at computation and quantitative analysis but are not able to perform the qualitative analysis required for fair-use analysis.[175] Sawyer pointed out that, among the four-step analysis of fair use, the first two factors, "purpose and character of the use" and "nature of the copyrighted works,"[176] would require human evaluation instead of technology determination.[177] Even for the third factor, "the amount and substantiality of the portion used in relation to the copyrighted work as a whole,"[178] which requires primarily a quantitative analysis, qualitative factors may come into play, according to Professor Beebe's empirical study.[179] When addressing the last factor of fair use, "the effect of use upon the potential market for or value of the copyrighted work,"[180] Sawyer noted that since this determination would require information external to the work itself, it would be impossible for a computer or any artificial intelligence to make such a determination.[181]

Sawyer is certainly not alone in questioning the effectiveness of UGC Principles in accommodating fair use. The Electronic Frontier Foundation (EFF) later proposed the Fair Use Principles for User Generated Video Content in response to the UGC Principles.[182] The EFF's fair use principles recommend qualitative standards to evaluate fair use; however, there are a few major reasoning flaws under its recommendations.

For instance, EFF's principles recommend that content be blocked only if both the audio and video tracks match the same work and 90 percent or more of the uploaded content comes from a single work.[183] This standard is logically flawed because a three-minute clip of a two-hour movie, which might qualify for fair use, will be blocked because the uploaded material will match exactly the fingerprint in the reference material. On the other hand, an uploaded video consisting of three full-length movies appended together might not be blocked because it probably only matches one-third of the database in the reference material.

The EFF's fair use principles also recommend the preservation of notice and take-down procedures.[184] This standard adds nothing to the existing copyright legal regime, however, either under the DMCA or the Chinese 2006 Regulations except for delaying the process for copyright owners to police. One big challenge that content owners face under the current notice-take-down provision is that, by the time the infringing content is eventually removed, the copyrighted video might have already been viewed or downloaded millions of times and a copy of that video been further duplicated and distributed to an even wider audience. Therefore, the preservation of a notice-take-down provision with a fingerprint filtering technology will seriously undermine the enforcement efforts of both UGC sites and copyright owners.

Finally the EFF's fair use principles encourage dialogue between users and content owners with an informal "dolphin" hotline to resolve fair-use take-downs.[185] This is a good proposal that will help to address the remedy issue in case of an erroneous blocking.

As correctly pointed out by the Shanghai High Court in *Zhongkai Culture v. Shulian Software,* the duty of care that is imposed on an ISP should be equivalent to the infringement risk that its business model carries.[186] In light of the Web 2.0 movement and the current business models for Chinese UGC sites, it is fair to ask Chinese UGC sites to share the enforcement burden with copyright owners to police copyright. This could be done either by encouraging a UGC Principle type of voluntary agreement signed between Chinese UGC sites and content owners or with less ambiguity and more binding power by imposing a mandatory filtering requirement for UGC sites before they can claim safe-harbor protection.

Graduated Response

The discussion related to fingerprint filtering concerns only hosting UGC sites. There are other online piracy challenges facing copyright owners, however, including through P2P file sharing services. These other challenges have led to the introduction of the GR program.

The GR program is also known as the three strikes policy. End-users who keep ignoring repeated notices on copyright infringement risk losing access to the Internet. The GR program was originally initiated in France (Elysee/Olivenness Agreement)[187] as a result of a three-way deal between the government, ISPs, and rights holders. To date, jurisdictions around the world including Taiwan[188] and South Korea[189] have enacted GR laws. Others jurisdictions including France, UK, Australia, New Zealand, Singapore, and the United States[190] are working toward implementing such rules either in law or in practice. The GR programs adopted in different jurisdictions have interesting variations.

GR Program in France

The French version of GR, known as HADOPI Law or *Creation and Internet Law*,[191] was introduced in 2009. The law attempts to regulate and control Internet access as a means of encouraging compliance with copyright laws. HADOPI is the government agency created by the law to police Internet users.[192] The French National Assembly first rejected the HADOPI bill on April 9, 2009, but the French government asked for reconsideration of the bill. The French National Assembly then adopted it on May 12, 2009,[193] and the French Senate adopted it on May 13. One central but controversial portion of the bill was struck down by the Constitutional Council on June 10, 2009, however. The Constitutional Council held that, because "the internet is a component of the freedom of expression" and "in French law the presumption of innocence prevails," only a *judge* can impose sanctions under the law.[194]

On October 22, 2009, the Constitutional Council approved a revised version of HADOPI, the Hadopi 2 bill (again including sanctions in a graduated response), which requires judicial review before revoking a person's Internet access, but that otherwise resembles the original requirements.[195]

GR Program in South Korea

In South Korea, the due process required before revoking the end-user's Internet subscription service is processed by an administrative agency, the Korea Copyright Commission (KCC), rather than a judicial court.[196] KCC was established to conduct mediation of disputes on copyright infringement. It may also deliberate on copyright infringement and injunction requests.

The three strikes legislation implemented in Korea targets not only end-users who repeatedly reproduce or upload unauthorized copyrighted content[197] but also message boards that receive more than three warnings and yet still do not carry out deletion orders, provided that such message boards are deemed to have impaired the "healthy use culture" of copyrighted works over the Internet.[198]

GR Program in Taiwan

The amendments to Taiwan's Copyright Law in May 2009 mandated a three strike policy on ISPs against their customers with respect to the customers' copyright infringement. The Taiwan Intellectual Property Office (TIPO) subsequently issued Implementing Regulations in November 2009.[199] Based on the Revised Copyright Law and Implementing Regulations, safe harbor provisions will be denied to ISPs if they fail to implement the three-strike infringement requirement. Therefore, in a P2P context, if an ISP fails to forward rightsholder's notices of initial and repeat infringements or to terminate (in whole or in part) the subscription of a repeat infringer following the third instance of infringement, it will be deprived of safe harbor protection.

TIPO fails to specify, however, how the three strike policy should be implemented. Based on TIPO's early drafts, it seems that the government will not be involved in enforcing the policy.[200] Rather, the policy will be considered a contractual agreement between an ISP and its end-users. As such, it will be the ISP that decides how to implement the policy, including how to determine the infringement activities and the accounts of the infringers and when to stop all or partial services, for example. This ambiguity has raised concerns as to the effectiveness of the implementation of the policy and different treatment that might be adopted by ISPs.

GR Proposal for China

Copyright violation through P2P file sharing is also very common in China. The government may consider adopting a GR program in China to prevent online piracy in the P2P context. The review body could be either a judicial court or an administrative agency to ensure due process. Repeated infringers who keep ignoring notices should be sanctioned with whole or partial termination of access to the Internet.

Conclusion

Online piracy has become one of the primary concerns for copyright holders in recent years as many users freely upload and distribute copyrighted content over the Internet without authorization. Instead of suing individual users, copyright owners have chosen to go after ISPs that provide services to end-users on secondary or joint liability theories. Although most jurisdictions including China and the United States have adopted relevant regulations to address the liability issue of ISPs, we have seen conflicting opinions in the interpretation and application of such regulations.

To better fight against online piracy, a number of recommendations have been proposed in response to specific technical features of ISPs that act as intermediaries of infringement activities. For instance, filtering technology might be a good cure for copyright violations using UGC services; GR programs, on the other hand, would be better suited to deter piracy using P2P file sharing services. Although critics might be concerned with fair use, privacy, and other possible abuses, a well-designed mechanism, such as a GR program equipped with due process, will strike a good balance between the interests of rights holders and the public, thus eventually promoting innovation and the public good.

Notes

1. An ISP is generally defined as "a provider of online services or network access, or the operator of facilities therefore," and an "entity offering the transmission, routing, or providing of connections for digital online communications, between or among points specified by a user, of material of the user's choosing, without modification to the content of the material as sent or received." *See* 17 U.S.C. §512(k)(1).
2. The term "China" in this article refers to the jurisdiction of People's Republic of China only and does not cover Hong Kong, Macau, or Taiwan.
3. To clarify, copyright infringement by individual users discussed in this article is restricted to unauthorized wholesale copying and time-shift recording of copyrighted works only, where end-users may upload full-length movies or TV episodes/programming and further distribute them over the Internet either through P2P file-sharing or user-generated content services without adding any creativity of their own. This article does not intend to discuss remixing or mash-up of copyrighted materials, which might involve more fact-specific fair use analysis.
4. *See* 3 Melville B. Nimmer & David Nimmer, Nimmer on Copyright, §12B.01[A] (2002), discussing the difficulty in determining which party should be liable for copyright infringement on the Internet: the poster, the users accessing the material, or the service provider making access possible.
5. *See id*. §12B.01[B][2].
6. The 1998 Digital Millennium Copyright Act (DMCA) is a US copyright law that implements two 1996 treaties of the WIPO.
7. NCR Corp. v. Korala Assocs., Ltd., 512 F.3d 807, at 816 (6th Cir. 2008).
8. Gershwin Publ'g Corp. v. Columbia Arts Mgmt., Inc., 443 F.2d 1159, 1166 (2d Cir. 1971). *See also* Shapiro, Bernstein Co. v. H.L. Green Co., 316 F.2d 304, 308 (2d Cir. 1963); CoStar Group, Inc. v. LoopNet, Inc., 373 F.3d 544, 550 (4th Cir. 2004).
9. MGM v. Grokster, 125 S. Ct. 2764 (2005).
10. *See Grokster*, 125 S. Ct. at 18.
11. *Id*. at 23.
12. *See id*. at 23.
13. 17 U.S.C. §512(a). The Transitory Network Communications Safe Harbor protects ISPs that are *passive conduits* from liability for copyright infringement, even if infringing traffic passes through their networks. In other words, if the infringing material is being transmitted at the request of a third party to a designated recipient, or handled by an automated process without human intervention, and is not modified in any way and only temporarily stored on the system, the ISP should not be held liable for the transmission.
14. 17 U.S.C. §512(b). The System Caching Safe Harbor protects ISPs who engage in caching (*i.e.*, creating copies of material for faster access) if the caching is conducted in standard ways, and does not interfere with reasonable copy protection systems. This section applies to the proxy and caching servers used by ISPs and many other providers. If the cached material is made available to end users, then the ISP must follow the Section 512(c) takedown and put back provisions. Note that this provision only applies to cached material originated by a third party, not by the provider itself (which otherwise will be direct infringement by ISP). Also, the content of the material must not be modified as a result of the caching process.
15. 17 U.S.C. §512(c). This provision on the storage of material on behalf of users (hosting) applies to ISPs that host infringing material for end-users.
16. 17 U.S.C. §512(d). The Information Location Tools Safe Harbor eliminates copyright liability for an ISP that links users, through a tool such as a Web search engine, to an online location that contains infringing material, provided that the ISP does not have actual or constructive knowledge that the material or activity is infringing. There are several other conditions for this immunity to apply. For instance, once the ISP becomes aware that the material is infringing, it must promptly disable access to it. Also, the ISP must follow §512(c)'s take-down and put-back provisions. Finally, when the ISP has the right and

ability to control the infringing activity, it must not receive financial benefit directly attributable to such activity.

17. 17 U.S.C. §512(i)(1)(A).
18. 17 U.S.C. §512(i)(1)(A).
19. 17 U.S.C. §512(i)(1)(B).
20. The same language in §512(c)(1)(B) can also be found in §52(d)(2), which discusses safe harbor for ISPs providing linking services.
21. For a comprehensive discussion of the debate on this issue, *see* Edward Lee, "Decoding the DMCA Safe Harbors," 32 *Colum. J.L. & Arts* 233 (2009).
22. *NCR Corp.*, 512 F. 3d at 816.
23. 17 U.S.C. §512(c)(3)(A)(iii).
24. 17 U.S.C. §512(c)(3)(B)(ii).
25. 17 U.S.C. §512(c)(1)(C).
26. Perfect 10, Inc. v. CCBill, LLC, 488 F.3d 1102 (9th Cir. 2007).
27. *Perfect 10,* 488 F.3d at 1108.
28. *Id.* at 1113.
29. *Id.* at 1113.
30. *Id.* at 1113.
31. Hendrickson v. eBay, 165 F. Supp. 2d 1082 (C.D. Cal. 2001).
32. *See* 165 F. Supp. 2d at 1084-1086.
33. *Hendrickson*, 165 F. Supp. 2d at 1089.
34. ALS Scan, Inc. v. Remarq Cmtys, Inc., 239 F.3d 619 (4th Cir. 2001).
35. *Id.* at 622 and 624. ALS Scan's notice directed the defendant RemarQ to two newsgroups containing infringing copies of its image, but not all materials at the offending sites belonged to ALS Scan.
36. *Id.* at 625.
37. H.R. Rep. No. 105-551, at 53 (1998).
38. 17 U.S.C. §512(c)(1)(A)(ii).
39. H.R. Rep. No. 105-551, at 53 (1998).
40. *Perfect 10*, 488 F.3d at 1114.
41. In re Aimster Copyright Litigation, 334 F.3d 643 (7th Cir. 2003).
42. *Id.*
43. *See Perfect 10,* 488 F.3d at 1117.
44. A&M Records v. Napster, 239 F.3d 1004 (9th Cir. 2001).
45. *See Napster*, 239 F.3d at 1023.
46. H.R. Rep. No. 105-551, pt. 2 at 54 (1998).
47. *Perfect 10,* 488 F.3d at 1118.
48. Ellison v. Robertson, 357 F.3d 1072 (9th Cir. 2004).
49. *Id.* at 1079.
50. *Id.*
51. *See Napster*, 239 F.3d at 1027.
52. *Hendrickson*, 165 F. Supp. 2d at 1093-1094.
53. *See id.*
54. *Napster*, 239 F.3d 1004.
55. Napster eventually declared bankruptcy and was liquidated before any final ruling on liability.
56. *See Napster*, 239 F.3d at 1020 n. 5.
57. *See Napster*, 239 F.3d at 1027.
58. *See Napster*, 239 F.3d at 1023.
59. In re Aimster Copyright Litigation, 334 F.3d 643 (7th Cir. 2003).
60. The *Aimster* court also discussed the Betamax defense in the *Sony* case and concluded that Aimster had failed to introduce any evidence of non-infringing use. *See* Sony Corp. v. Universal City Studios, Inc., 464 U.S. 417 (1984).
61. *See Aimster*, 334 F.3d at 3.
62. *See Aimster*, 334 F.3d at 11.
63. *See Aimster*, at 11.
64. *See Aimster*, 334 F.3d at 21, referring to 17 U.S.C. §512(i)(1)(A).
65. *Id.*
66. *Grokster*, 125 S. Ct. 2764 (2005).
67. *Id.*
68. *Id.*
69. *Id.*
70. *Id.*
71. *Id.*
72. *Id.*
73. *Id.*
74. *See* IO Group Inc. v. Veoh Networks, Inc., 586 F. Supp. 2d 1132 (N.D. Cal. 2008), available at *http://docs.justia.com/cases/federal/district-courts/california/candce/5:2006cv03926/181461/117/.*
75. *Id.* (Emphasis added).
76. *Id.*
77. *Id.* With regard to the red flag test, *i.e.*, "apparent infringing activity," the Court held that, because none of the allegedly infringing video files uploaded by Veoh's users contained IO Group's copyright notices, Veoh did not have constructive knowledge either.
78. *See* Corbis Corp. v. Amazon.com, Inc., 351 F. Supp. 2d 1090 (W.D. Wa. 2004).
79. *See Veoh*, 586 F. Supp. 2d at 21.
80. *See id.* at 23.
81. *See id.* at 25-26.
82. Viacom Intern. Inc. v. YouTube Inc., 540 F. Supp. 2d 461 (S.D.N.Y. 2008).
83. *See* Complaint at 48-97, Viacom v. YouTube, Inc., No. 1:07-cv-02103 (S.D.N.Y. Mar. 14, 2007).
84. European Union E-commerce Directive 2000/31/EC.
85. *See* Article 17, E-commerce Directive, full text available at *http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32000L0031:en:NOT.*
86. *See* Preamble 40, E-commerce Directive.
87. *See* Andrea Schultz, Legal Aspects of An Ecommerce Transaction 42, (2006). The corresponding US legislation can be found at CF CDA §230.
88. *See* EU E-commerce Directive, Articles 12 and 13.
89. *See* EU E-commerce Directive, Article 14.

90. *See id.*, Article 15.
91. *See* B. Spitz, "The Buttock Sues MySpace for Copyright Infringement," *http://www.juriscom.net/actu/visu.php?ID=942*, Nov. 7, 2007.
92. In France, the publisher of printed matter or audiovisual content is held liable merely on the finding of an infringement according to Article 42 of the *Loi du 29 juillet 1881 sur la libete de la presse* (Act on Freedom of the Press of 29 July 1881).
93. *See* B. Spitz, "The Buttock Sues MySpace for Copyright Infringement," *http://www.juriscom.net/actu/visu.php?ID=942*, Nov. 7, 2007.
94. Christian, C., Nord Quest Production v. DailyMotion, UGC Images, Tribunal de Grande Instance de Paris (3d chamber, 2d Section) decision of July 13, 2007, *http://www.juriscom.net/actu/visu.php?ID=949*. July 2007.
95. *See id.*
96. *See id.*
97. Under French law, liability of ISPs is governed by the EC Directive on Electronic Commerce n°2000/31, dated June 8, 2000, and the French Law n°2004-575, dated June 21, 2004, and called *Loi pour la confiance dans l'économie numérique* (LCEN). Article 6-I-2 LCEN provides that "hosting providers may not be held civilly liable for the activities or information stored at the request of a recipient [i.e. user] of these services if they did not have actual knowledge of their unlawful nature or of facts and circumstances making this nature apparent, or if, as soon as they obtained such knowledge, they acted expeditiously to remove or to disable access to these data."
98. *See* Christian, C., Nord Quest Production v. DailyMotion, UGC Images, Tribunal de Grande Instance de Paris (3d chamber, 2d Section) decision of July 13, 2007, *http://www.juriscom.net/actu/visu.php?ID=949*. July 2007.
99. *Id.*
100. DailyMotion, "DailyMotion Selects Audible Magic's Fingerprinting Solution for Detecting Copyrighted Video," (May 10, 2007), available at *http://www.dailymotion.com/press/AudibleMagic.pdf*.
101. *See* Lancôme Parfums et Beautie & Cie v. eBay International AG, eBay Europe S.A.R.L., eBay, Belguim, 2008, A/07/06032.
102. Lancôme ordered almost 100 perfumes bearing its trademark from the auctioneer Web site *www.ebay.com* to measure the scale of counterfeits on the Internet. It turned out that 77 perfumes that it ordered out of 85 were counterfeits. *See id.*
103. *See* Lancôme Parfums et Beautie & Cie v. eBay International AG, eBay Europe S.A.R.L., eBay, Belgium, 2008, A/07/06032.
104. *See* Lancôme v. eBay, Belgium 2008, A/07/06032.
105. SARL Zadig Productions, Jean-Robert Viallet et Mathieu Verboud v. Ste Google Inc. et AFA, Tribunal de Grande Instance de Paris (3d Chambre, 2d Section), decision of Oct. 19, 2007. *http://www.juriscom.net/actu/visu.php?ID=976*.
106. *See id.*
107. B. Spitz, "Google Video held liable for not doing all it could to stop the broadcasting of a film," Nov. 29, 2007. *See http://copyrightfrance.blogspot.com/2007/07/dailymotion-hosting-provider-liable-for.html*.
108. SA Scarlet v. SABAM, Tribunal de Premiere Instance de Bruxelles, 22 Oct. 2008.
109. *See* "Court Rules against RapidShare in Germany," June 25, 2009, *http://www.afterdawn.com/news/archive/18292.cfm*. As part of the ruling, the court ordered RapidShare to "proactively filter" more than 5,000 tracks from GEMA (The German Copyright Society) catalogue. The case is under appeal now.
110. *See* "Court Jails Pirate Bay Founders," *BBC News*, Apr. 17, 2009, available at *http://news.bbc.co.uk/2/hi/technology/8003799.stm*. Pirate Bay was later seeking a retrial on the grounds of conflict of interests and bias, but was denied by Swedish Appeal Court. *See* "Swedish Appeals Court Denies Pirate Bay Retrial—Says No Bias By Judge," available at *http://www.techdirt.com/articles/20090625/0949185362.shtml*.
111. *See* Articles 10, 37, 41, and 47 of the PRC Copyright Law. Full text is available at *http://www.chinaiprlaw.com/english/laws/laws10.htm*.
112. English translation of the Regulations is available at *http://www.cpahkltd.com/Archives/063A-p90.Pdf*.
113. *See* Article 130 "Joint-Liability" theory defined under The General Principles of the Civil Law of the PRC (The Civil Law, 1987).
114. The Chinese Tort Law was passed on Dec. 26, 2008, and will come into effect on July 1, 2010. *See* Articles 9 and 36 of the PRC Tort Law.
115. Article 4 of the Interpretations of the Supreme People's Court of Several Issues Regarding Applicable Laws for the Hearing of Copyright Disputes Involving Computer Networks.
116. Articles 22 and 23 of the Regulations.
117. Judge CHEN Jing chuan, the Chief Judge at Beijing High Court, made the aforesaid remarks at "Sino-US Roundtable for Copyright Protection over the Internet" on Dec. 18, 2009, in Beijing.
118. Columbia Pictures v. Sohu.com, Beijing First Intermediate Court, 27 Dec. 2006. *See* Yi Zhong Min Chu Zi No. 11932 (2006).
119. *See id.* at 1.
120. *See id.* at 5.
121. Ningbo Success Media Communications Ltd. v. Beijing Alibaba Information Technology Ltd., decided by Beijing No. 2 Intermediate Court, (2008) Er Zhong Min Zi Di 19082.
122. *See id.* at 1.
123. *See id.* at 1.
124. *See id.* at 2.
125. *See id.* at 3.
126. *See id.* at 3.
127. *See id.* at 3-4.
128. *See id.* at 3-4.
129. IFPI v. Baidu (The Beijing First Intermediate Court, 2005 No. 7965), (2005) yi zhong min chu zi di 7965 hao. This ruling was affirmed by the Beijing High Court in 2007. *See* IFPI v. Baidu (Beijing High Court, 2007 No. 594), 2007 gaomin zhongzi di 594 hao.

130. *See IFPI*, at. 2-3.
131. *See id.* at 16-17.
132. *See id.* at 3.
133. *See* IFPI v. Baidu (Beijing High Court, 2007 No. 594), 2007 gaomin zhongzi di 594 hao.
134. IFPI v. Alibaba (The Beijing High Court, 2007 No. 1190), 2007 Gao Min Zhong Zi Di 1990 Hao.
135. *See id.* at 9.
136. *See id.* at 33.
137. *See id.* at 33.
138. Article 26 of the Regulations defines "rights of communication through information network" as "rights of communicating a work, performance, sound recording or video recording to the public, by wire or wireless means, where members of the public may access to these works *from a place and at a time individually chosen by them*."
139. *See Alibaba,* (The Beijing First Intermediate Court, 2005 No. 7965), (2005) yi zhong min chu zi di 7965 hao.
140. *See id.*
141. In *Alibaba,* IFPI's take-down notice includes a list of 34 singers and 48 CDs that might have been infringed, and a few sample URL addresses linking to 136 infringing songs.
142. Article 22.
143. Article 24 (Emphasis added).
144 *See Alibaba*.
145. Guangdong Zhongkai Culture Development Ltd. v. Guangzhou Shulian Software Technology Ltd. (2008, No. 7 Shanghai High Court) 2008 Hugaominsan zhi zhongzi di 7 hao.
146. *Id.* at 8.
147. *Id.* at 9.
148. *Id.* at 8.
149. *Id.* at 9.
150. *Id. at* 9.
151. IFPI sent out its first take-down notice to Alibaba on July 4, 2006, requiring removal of all infringing links related to the songs identified in its notice within seven days of the receipt of the notice. IFPI then made follow-up calls and written inquiries on July 20, July 28, August 3, and August 10, respectively. Alibaba admitted that it did not delete all infringing links until August 3, 2006. *See* IFPI v. Baidu (The Beijing High Court, 2007 No. 1190), 2007 Gao Min Zhong Zi Di 1990 Hao, at 23-24.
152. Liu Jingsheng v. Sohu Aite Technology Ltd. (Beijing Second Intermediate Court, Dec. 2000).
153. *See id.* at 2.
154. *See id.* at 2.
155. The "24-48 hour" requirement for responding to a take-down notice has been frequently requested by content industries, including MPAA in its recent submissions to legislators in various countries.
156. Emphasis added.
157. Article 8 of WCT provides that, "Without prejudice to the provisions of Articles 11(1)(ii), 11*bis*(1)(i) and (ii), 11*ter*(1)(ii), 14(1)(ii), and 14*bis*(1) of the Berne Convention, authors of literary and artistic works shall enjoy the exclusive right of authorizing any communication to the public of their works, by wire or wireless means, including the making available to the public of their works in such a way that members of the public may access these works from a place and at a time individually chosen by them." There seems to be a consensus that the word "including" in this Article suggests that both on-demand and real-time retransmission services are covered under this Provision. Full text is available at *http://www.wipo.int/treaties/en/ip/wct/trtdocs_wo033.html#P78_9739*.
158. Principles for User Generated Content Services, *http://ugcprinciples.com/* (last visited on 1/16/09).
159. Peter Menell and David Nimmer, "Unwinding *Sony*," *California L. Rev.* Vol. 95:941, at 1006 (2007).
160. The authors made an analogy between joint and several liability theories under tort law principles to contributory (and inducement) liability theory under copyright law, finding that both theories include elements of "intent" and "knowledge" of infringement activities. Similarly, the authors believe that vicarious liability under copyright law also fits into the agency/enterprise branch of indirect tort liability. *See* more discussion on this topic at 1012-1014.
161. *Id.* at 1016.
162. *Id.* at 1006, quoting a wider range of literature discussing the least cost avoider and other theories. *See* Guido Calabresi, "Some Thoughts on Risk Distribution and the Law of Torts," 70 *Yale L.J.* 499 (1961); William M. Landes & Richard A. Posner, The Economic Structure of Tort Law (1987); Steven Shavell, Economic Analysis of Accident Law (1987). *See also* Restatement (Third) Torts: Prod. Liab. § 2, reporter's notes, cmt. a (1998) (citing James Henderson, Jr. & Aaron D. Twerski, "Closing the American Products Liability Frontier: The Rejection of Liability Without Defect," 66 *N.Y.U. L. Rev.* 1263 (1991).
163. *Id.* at 1017.
164. Quoting language from *Napster*, 239 F. 3d at 1023.
165. Principles for User Generated Content Services, *http://ugcprinciples.com/* (last visited on 1/16/09).
166. *See id.* Article 3.
167. Content owners may set out certain specifications such as allowing the upload of short clips no more than five minutes to accommodate fair use.
168. *See id.* Article 3 (e).
169. *See id.* Article 3 (d).
170. BBC, "YouTube Rolls out Filtering Tools," 16 Oct. 2007, available at *http://news.bbc.co.uk/2/hi/technology/7046916.stm* (last visited on 1/17/10).
171. DailyMotion installed the Audible Magic Fingerprint technology on its Web site after it lost the case *Joyeux Noel*. *See* DailyMotion, "DailyMotion Selects Audible Magic's Fingerprinting Solution for Detecting Copyrighted Video," (May 10, 2007).
172. Vobile was developed by a Chinese vendor and was tested during the 2008 Beijing Olympic Games to prevent unauthorized retransmission of sports games over the Internet.

173. Enswer is a fingerprint technology developed by a Korean vendor.
174. *Youku.com*, one of the largest UGC sites in China, claims on its Web page that it is developing its own fingerprint filtering technology to protect copyrighted materials although it has been sued by a number of proprietors in the second half of 2009 for copyright infringement. *See http://www.youku.com/about/en/faq/*. (last visited on 1/17/10). *Also see* "Youku Fined for Copyright Infringement," published at Media Asia on Nov. 30, 2009, at *http://www.media.asia/searcharticle/UPDATE-Youku-fined-for-copyright-infringement/2008/38065?src=related*.
175. Michael S. Sawyer, "Filters, Fair Use and Feedback: User-Generated Content Principles and the DMCA," *Berkeley Technology L. J.* 24:1 (2009), at 29.
176. 17 U.S.C. § 107 (2006).
177. *See* Michael S. Sawyer, *supra* note 175, at 29.
178. 17 U.S.C. § 107 (2006).
179. *See* Michael S. Sawyer, *supra* note 175, at 29. Sawyer quoted Professor Beebe's empirical fair use study showing that, when an entire copyrighted work was copied, courts still found fair use 27 percent of the time. *See* Barton Bee, "An Empirical Study of US Copyright Fair Use Opinions," 156 *U. Pa. L. Rev.* 549, 616 (2008).
180. 17 U.S.C. § 107 (2006).
181. *See* Michael S. Sawyer, *supra* n.177, at 30.
182. The Electronic Frontier Foundation, "Fair Use Principles for User Generated Video Content," available at *http://www.eff.org/issues/ip-and-free-speech/fair-use-principles-usergen* (last visited on 1/17/10), hereinafter referred to as Fair Use Principles.
183. *Id*. at 2(a).
184. *See id*, at. 3.
185. It is called a "dolphin" hotline because fair use is caught in an infringement dilemma just as dolphins are caught in a fishing net. *See id*.
186. *See* Zhongkai Culture, at 9.
187. *Accord pour le développement et la protection des œuvres et programmes culturels sur les nouveaux réseaux,* vendredi 23 novembre 2007, available at *http://www.culture.gouv.fr/culture/actualites/conferen/albanel/accordolivennes.htm*.
188. The enactment of amendments to Taiwan's Copyright Law in May 2009 mandated a three-strike policy on ISPs against their customers in respect of copyright infringement. Taiwan's Intellectual Property Office (TIPO) subsequently issued Draft Implementing Regulations in November 2009. *See* Article 90 (4) of Taiwan Copyright Act, *http://www.tipo.gov.tw/en/AllInOne_Show.aspx?path=2557&guid=26944d88-de19-4d63-b89f-864d2bdb2dac&lang=en-us*.
189. The amended Copyright Law of South Korea became effective on July 23, 2009. Article 133-2 is a "GR program" as proposed by the Ministry of Culture, Sports and Tourism of the South Korea (MSCT).
190. "Verizon ends service of alleged illegal downloaders," Jan. 20, 2010, *http://news.cnet.com/8301-1023_3-10437176-93.html?tag=TOCmoreStories.*
191. In French Loi Favorisant la diffusion et la protection de la creation sur Internet. French Senate. *http://www.senat.fr/dossierleg/pjl07-405.html*.
192. HADOPI is the abbreviation of the government agency "Haute Autorite pour la Diffusion des Oeuvres et la Protection des Droits sur Internet" (High Authority of Diffusion of the Art Works and Protection of the Copyrights on Internet).
193. France 24, "Lawmakers adopt Internet anti-piracy bill," May 12, 2009, *http://www.france24.com/en/20090512-lawmakers-adopt-internet-anti-piracy-bill-illegal-downloading-France.*
194. France 24, "Top legal body strikes down anti-piracy law," June 10, 2009, *http://www.france24.com/en/20090610-top-legal-body-strikes-down-anti-piracy-law-hadopi-constitutional-council-internet-france* (emphasis added).
195. Pfanner Eric, "France Approves Wide Crackdown on Net Piracy," *NY Times*, Oct. 22, 2009, available at *http://www.nytimes.com/2009/10/23/technology/23net.html*.
196. *See* Article 133-2, Revised Korean Copyright Act, July 2009. Paragraph 1 provides that if illegal reproductions are transmitted through means of information and communication network, MCST may order the relevant OSP to: (i) give a warning notice to reproduce and/or transmitter of the reproduction and/or (ii) delete or stop the transmission of the reproduction, after the deliberation of the Korean Copyright Commission (KCC).
197. *See id*. Paragraph 2 of Article 133-2. Paragraph 2 of Article 133-2 provides that if MCST finds that a same reproducer and/or transmitter, who had already been given the warning notice of above (i) for more than three times, continues such unauthorized transmission, then the MCST may order the OSP to suspend his account for a period designated no more than six months, after the deliberation of the Korean Copyright Commission (KCC).
198. *See id*. Paragraph 4 of Article 133-2. Paragraph 4 provides that if MCST finds an online bulletin board that has already received the warning notices more than three times, yet continues to disturb public order, MCST may order the OSP to suspend the account related to illegal reproduction and/or transmission, for a period designated no more than 6 months, after the deliberation of the KCC.
199. *See* Article 90 (4) of Taiwan Copyright Act, at *http://www.tipo.gov.tw/en/AllInOne_Show.aspx?path=2557&guid=26944d88-de19-4d63-b89f-864d2bdb2dac&lang=en-us.*
200. *See* IIPA—AIWAN 2010 Special 301 Report on Copyright Protection and Enforcement, at 4, available at *http://www.iipa.com/rbc/2010/2010SPEC301TAIWAN.pdf.*

Reprinted from *The Computer & Internet Lawyer*, July 2010, Volume 27, Number 7, pages 7 to 24, with permission from Aspen Publishers, Inc., a Wolters Kluwer business, New York, NY, 1-800-638-8437, *www.aspenpublishers.com*.