

ISP Liability under the Copyright Law Regime in China

By Seagull Haiyan Song

How to determine the liability of Internet service providers (ISPs) has become one of the most debated issues of Internet law and policy. This article will primarily address ISP liability under the copyright law regime in China: under what circumstances should ISPs be held liable when copyrighted material is transmitted, or made available, over the Internet without authorisation of copyright holders.¹ Meanwhile, this 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.

ISPs might become vulnerable to charges of copyright infringement, whether direct or indirect, in 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 cyberspace.² There have been no universally accepted secondary liability theories worldwide. Nonetheless, an overall review of copyright infringement cases in China shows that the courts will generally consider the following factors when determining the liability on 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.

Chinese ISP legislation

The existing Chinese copyright law provides certain protection to copyright owners in the digital world.³ China adopted the Regulations for the Protection of Rights of Communication through Information Networks (2006 Regulations)⁴ to address increasing concerns over online piracy. The 2006 Regulations follow a number of principles set out in the DM-CA, including the safe harbour provisions for ISPs.⁵

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 immunises 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 direct infringement by its end-users in China lies in its Civil Code⁶ and the recently enacted PRC Tort Law⁷ and its joint-liability theory. The Supreme People's Court's 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 Application of Law to Trial 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.⁸

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, intent, ability and rights to control infringing activity, financial benefits arising from infringing activities, and contribution to the infringing activity, to mention just a few.⁹

ISP liability cases in China

ISP's direct liability

In *Columbia Pictures v. Sohu.com*,¹⁰ Columbia Pictures filed a lawsuit against Sohu for copyright infringement after discovering that Sohu had provided subscription-based access to an unauthorised online video archive of approximately 100 US films. The archive included films produced by Columbia Pictures and other studios. The Beijing No.1 Intermediate Court accepted Columbia Pictures' claims.

ISP's indirect liability

ISPs providing "hosting" services (Article 22)

In *Success Media v. Alibaba*,¹¹ 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 authorisation.

Alibaba argued that the safe harbour provision of Arti-

cle 22 (hosting service) 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. Alibaba further argued that it had 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.

The Beijing Chaoyang District Court accepted Alibaba's arguments, and held Alibaba not liable for the copyright infringement. 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 the copyright infringement on the ground that Alibaba knew or had had reasonable grounds to know that the uploaded content was infringing. 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. Moreover, Alibaba had provided a detailed introduction of the TV series, including posters, cast ,directors, and synopsis, for example, on its home page. Therefore, the defendant knew or had reasonable grounds to know that the uploaded TV episodes were provided by its users without authorisation. As such, the Article 22 safe harbor provision didn't apply, and Alibaba was held liable for copyright infringement.

ISPs providing "searching/linking" services (Article 23)

In *IFPI v. Baidu*,¹² 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. The Beijing No. 1 Intermediate Court agreed with Baidu's arguments, acknowledged Baidu's status as a linking service provider, and ruled that the safe harbour provision of Article 23 should apply.

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. The Beijing Higher Court later affirmed the Intermediate Court's decision.¹³

In a similar copyright infringement case brought six months later by the same plaintiff against a similar defendant, however, the search engine Alibaba/cn.yahoo.com, the

same Beijing Higher Court came to an entirely different conclusion, finding 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 Higher Court dismissed the plaintiff's direct liability claim on the grounds that Alibaba was providing only the "searching/linking services" and was not directly liable for copyright infringement.

When addressing the indirect liability claim, the court 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. 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, and thus was jointly liable for copyright infringement.¹⁴

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 harbour provisions of Article 10-23 under the 2006 Regulations. Moreover, since the 2006 Regulations were drafted to address only the video-on-demand (VOD) services,¹⁵ and do not cover real-time retransmission of copyrighted works over the Internet, there seems to be a lack of legal basis for preventing unauthorised 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 No. 1 Intermediate People's 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 takedown notice.¹⁶ In IFPI v. Alibaba, 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.¹⁷

In IFPI v. Alibaba¹⁸, however, the Beijing No.2 Intermediate People's 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,¹⁹ 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 harbour protection, the 2006 Regulations consider knowledge a factor when analysing 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" (Article 22). Similarly, an ISP providing linking/searching services cannot claim safe harbour protection if "it knows or should know that the linked works, performances, sound recordings ... infringe another party's rights" (Article 24).

Nonetheless, it is still unclear how the Chinese version of the red flag tests - 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.²⁰

Similarly, in Zhongkai Culture v. Shulian Software,²¹ the Shanghai Higher People's 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 19 November 2005, by its

end-users was unauthorised. 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. The court also took a more liberal view of the red flag test, that is, the infringing activity should have been apparent to any reasonable person under the same or similar circumstances.

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 harbour protection. In *Zhongkai Culture v. Shulian Software*, the Shanghai Higher People's Court specifically noted that "the duty of care that is imposed on an ISP should be equivalent to the infringement risks that its business models carry."²² 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."²³ 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.²⁴

In *Liu Jingsheng v. Sohu Aite Technology Ltd.*²⁵, 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 authorisation.

When addressing the indirect liability claim, 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.

It is unclear from the current legislation and case law exactly what constitutes "expeditiousness" of a takedown. Most content owners argue that, given the widespread effect of the Internet, where millions of views and downloads take

place within 24 hours after some 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.²⁶

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 the "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." In other words, the 2006 Regulations are drafted to deal with video-on-demand (VOD) services, and do not cover real-time unauthorised 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,²⁷ the WCT definition could be considered a legal basis for enforcement against 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. 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 residing in 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),²⁸ which was used to automatically block the unauthorised content on these UGC sites. 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

Both the DMCA and the 2006 Regulations have put the burden of policing the internet for copyright infringement on copyright owners, and ISPs must only cooperate when necessary to eliminate copyright infringement.²⁹ However, as Brandon Brown argued in his paper, this burden may be inequitable in light of the Web 2.0 movement, where the binary rules, i.e. whether an ISP profits directly, whether it has knowledge or ability to block access, etc., are blurring among UGC sites.³⁰ In other words, it is fair to ask 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 unauthorised uploading of infringing content on their sites.

The proposed fingerprint filtering technology under UGC Principles would allow an ISP to compare uploaded materials with samples of copyrighted materials (reference material) provided by copyright owners.³¹ If uploaded material matches any reference material and falls into the specifications pre-designed by content owners, the uploaded material will be blocked before it is uploaded unless it is licensed from the copyright owners, as identified in the “white list.” 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 authorised uploads; and (3) accommodating fair use.”³²

As it was correctly pointed out by the Shanghai Higher People’s 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. 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-harbour protection.

Graduated response

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/Olivrenness Agreement)³³ as a result of a three-way deal between the government, ISPs, and rights holders. To date, jurisdictions around the world, including Taiwan and South Korea, have enacted GR laws. Other jurisdictions, including France, UK, Australia, New Zealand, Singapore, and the United States, are now 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,³⁴ was introduced in 2009. 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.³⁵

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.³⁶

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.³⁷

The three strikes legislation implemented in South Korea targets not only end-users who repeatedly reproduce or upload unauthorised copyrighted content, 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.

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 the Implementing Regulations in November 2009.³⁸ Based on the Revised Copyright Law and the Implementing Regulations, safe harbour provisions will be denied

to ISPs if they fail to implement the three-strike infringement requirement.

However, the policy will be considered a contractual agreement between an ISP and its end-users. As such, it will be the ISP that decides on how to implement the policy, including how to determine 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.

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 Internet access. ■

The author: Senior IP Counsel at the Walt Disney Company Shanghai Office, former consultant with Arnold & Porter LLP and a former partner with King and Wood, member of the Chinese Bar Association, member of the California Bar Association, LL.M of Hong Kong University, LL.M and J.S.D of UC Berkeley School of Law (Boalt Hall)

¹ 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.

² See 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.

³ See Articles 10, 37, 41, and 47 of the PRC Copyright Law.

⁴ English translation of the Regulations is available at <http://www.cpahkltd.com/Archives/063A-p90.Pdf>.

⁵ DMCA § 512 provides that an ISP might be exempt from liability for copyright infringement stemming from transmitting, caching, hosting, or linking to infringing materials. To trigger the safe harbour provisions, an ISP must satisfy two threshold requirements. First, the ISP must “adopt and reasonably implement a policy” of addressing and terminating ac-

counts of users who are “repeat infringers.” Second, the ISP must accommodate and not interfere with “standard technical measures.” 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.

⁶ See Article 130 “Joint-liability” theory defined under the General Principles of the Civil Law of the PRC (The Civil Law, 1987).

⁷ See Articles 9 and 36 of the Chinese Tort Law.

⁸ 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.

⁹ Articles 21, 22 and 23 of the Regulations.

¹⁰ Columbia Pictures v. Sohu.com, Beijing No.1 Intermediate People’s Court, 27 Dec. 2006. See No. Yizhongminchuzi 11932 /2006.

¹¹ Ningbo Success Media Communications Ltd. v. Beijing Alibaba Information Technology Ltd., the Beijing No. 2 Intermediate People’s Court, No. Erzhongminzi 19082/2008.

¹² IFPI v. Baidu, the Beijing No.1 Intermediate People’s Court, No.7965/2005, No. Yizhongminchuzi 7965/2005.

¹³ IFPI v. Baidu, the Beijing Higher People’s Court No. Gaominzhongzi 594/2007 .

¹⁴ IFPI v. Alibaba, the Beijing Higher People’s Court, No. Gaominzhongzi 1990/2007.

¹⁵ 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.”

¹⁶ Supra Note 12.

¹⁷ Supra Note 14.

¹⁸ IFPI v. Alibaba, the Beijing No. 2 Intermediate People’s Court, No. Erzhongminchuzi 2626/2007.

¹⁹ 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.

²⁰ Supra Note 18.

²¹ Guangdong Zhongkai Culture Development Ltd. v. Guangzhou Shulian Software Technology Ltd., the Shanghai Higher People’s Court, No. Hugaominsanzhizhongzi 7/2008.

²² Id.

²³ Supra Note 14.

²⁴ 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 Higher People's Court, No. Gaominzhongzi 1990/2007, Pp. 23-24.

²⁵ *Liu Jingsheng v. Sohu Aite Technology Ltd.* (Beijing Second Intermediate Court, Dec. 2000).

²⁶ 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.

²⁷ 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 14bis (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.

²⁸ Principles for User Generated Content Services, <http://ugcprinciples.com/>

²⁹ See 17. U.S.C. §512(2000) and articles 20-23 of 2006 Regulations.

³⁰ See Brandon Brown, *Fortifying the Safe Harbors: Reevaluating the DMCA in a Web 2.0 World*, 23 *Berkeley Tech. L. J.* 2008, at 463-465.

³¹ Content owners may set out certain specifications such as allowing the upload of short clips no more than five minutes to accommodate fair use.

³² Supra Note 28, Article 3.

³³ Accord pour le développement et la protection des oeuvres et programmes culturels sur les nouveaux réseaux, vendredi 23 novembre 2007, available at <http://www.culture.gouv.fr/culture/actualites/conferen/albanel/accordolivennes.htm>.

³⁴ In French Loi Favorisant la diffusion et la protection de la creation sur Internet. French Senate. <http://www.senat.fr/dossierleg/pj107-405.html>.

³⁵ France 24, "Top legal body strikes down anti-piracy law," June 10, 2009, <http://www.france24.com/en/20090610-top-legal-bodystrikes-down-anti-piracy-law-hadopi-constitutional-council-internetfrance>.

³⁶ 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>.

³⁷ See Article 133-2, Revised Korean Copyright Act, July 2009. Para-

graph 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).

³⁸ See Article 90 (4) of Taiwan Copyright Act, at http://www.tipo.gov.tw/en/AllInOne_Show.aspx?path=2557&guid=26944d88de19-4d63-b89f-864d2bdb2dac&lang=en-us.