Crossing the Pond: International ISP's and the Barrier Reef of Strict Liability[**]

By
Professor Doris Estelle Long[1]
The John Marshall Law School
Chicago, Ill 60604
7long@jmls.edu

Introduction

By its very nature, the internet[2] is one of the most global means of communication developed to date. No country is completely without the internet, even if its access is limited to a few government agencies and a handful of cybercafes in the capital city. Yet despite the critical importance of service providers, and the wide spread availability of the internet globally to end users, any service provider who decides to "cross the pond" of the internet will find the trip a sometimes dangerous and often uncharted one. Despite a relatively longstanding existence, at least in terms of technology, the internet and its content appears at times to be uncharted territory insofar as legal liability for unauthorized content is concerned. The "bad news" is that no international treaty currently exists which establishes a global standard for third party content liability. The "good news" is that international standards are emerging which should help service providers avoid at least some of the current liability shoals.

While this paper attempts to provide some general oversight regarding current international standards for ISP liability, particularly for third party content, it should be noted that domestic laws still differ greatly regarding such critical issues as the scope of safe harbors, and what qualifies as knowledge of illegal content sufficient to remove a safe harbor exemption. This paper can only provide a snapshot of some past and current developments in this constantly changing, yet critical, international arena. It is intended

---

[**] This article was originally published as part of the Conference Proceedings of the Annual Spring Conference of the AIPLA in May 2004.

[1] Doris Estelle Long is a Professor of Law at The John Marshall Law School in Chicago, Illinois where she specializes in intellectual property and internet law, including its international, technological and cultural implications. Professor Long would like to thank Adam Hicks whose research assistance proved invaluable in the initial stages of this paper.

[2] Although common usage continues to use initial capitals to describe "the Internet," such usage no longer seems appropriate given the internet's wide spread and long standing use. Just as "the Telephone" has become "the telephone," so too, it is time to recognize that "the Internet" has become an accepted and longstanding communication form which no longer needs to be treated with the exclamatory reverence of initial capital letters. Such special treatment, I believe, has been used in part to relieve international law of its responsibility to resolve the legal issues surrounding intellectual property on the internet. Capital letters subconsciously tell us all that the "Internet" is something new, so new that we cannot yet be expected to deal with the problems it poses. The time for such complacency, along with the initial capital letters, is long past.

to discuss some of the most important developments in the law, but is *not* intended to be a comprehensive discussion of all the issues and cases in the area. It is also *not* intended to take the place of research or consultation with appropriate legal personnel regarding the domestic laws of any particular country in which a party intends to act as a service provider.

In his book *The Victorian Internet*,[3] Tom Standage compares the issues facing today's internet with its technological equivalent of the 19th Century – the telegraph. Similar to the telegraph, the internet poses critical issues about who should be held accountable for the content of information which is communicated by unrelated third parties, yet without whose critical services the potential impact of such content would be largely unrealized. In the early 20th Century, similar issues arose with the introduction of the telephone. Like the problems posed by the telegraph, technological advances in communications media gave third party service providers (telephone companies) the ability to reap large financial rewards by assisting in the transmission of messages whose adverse impact could be greatly enhanced through their services.

In the early ages of the internet, courts looked to both of these analogues for acceptable legal doctrines. Yet the distinct differences between the telegraph and telephone, on one hand, and the internet on the other, make such analogues largely unhelpful, if not wholly irrelevant. At its most basic, only the internet, with the development of the World Wide Web, allows for the storage and subsequent transmission of illegal works to unknown (and probably unknowable) end users on a global scale.

Emerging International Standards

Internationally the development of international standards for ISP liability has followed the same "progressive exemption" approach of other IP liability issues on the internet. Probably the closest analogy to the development of international ISP liability standards is the development of liability standards for domain names composed of a well-known trademark and the "sucks" suffix. These cases began initially with an almost absolute prohibition against the unauthorized use of "sucks" marks, bolstered by a narrow application of trademark laws to the internet.[4] Over time, as the role of "suck" sites became better understood, courts and arbitrators began to recognize that a likelihood of confusion does not automatically arise simply because "suck" has been added to another's mark.[5] Liability exemptions in this area have become so well established, that it appears that there is a nearly absolute safe harbor for "suck" domains on the internet.[6] The development of international liability exemptions for ISP's has not developed quite so far as to recognize any *absolute* safe harbors but the trend is clearly toward a greater

[3] Tom Standage, *The Victorian Internet* (Berkeley Books 1998).
[4] *See, e.g., Wal_mart Stores, Inc. v. Harvey*, WIPO No. D-2000-1104 (Nov. 23, 2000)(Walmartsucks.com use prohibited).
[5] *See, e.g., Bloomberg LP v. Secaucus Group*, No. FA 0104000097079 (NAF upholds registration of bloombergsucks.com domain name).
[6] *Lucent Technologies Inc. v. Johnson*, 2000 WL 1604055 (C.D.Cal. 2000), however, demonstrates that the exemption is not complete since use of a "sucks" domain name on a site that displayed pornographic material can still be prohibited.

acknowledgement internationally that certain types of provider activity are worthy of safe harbor exemptions.

Liability Paradigms

In the area of content control over the internet there are three major categories of content for which different liability paradigms may be used. The first is the liability for content that is considered to be harmful to the reputations of individuals, such as under traditional defamation and slander laws. The second category is the liability for content that is considered to be harmful to the public order. This includes content that violates political or religious principles of the present government, or which is considered violative of public morals, such as in the case of works considered obscene, or harmful to minors. The third category concerns the liability for the dissemination of works that infringe intellectual property rights in general, and copyright specifically.

Liability paradigms for personal harms seems to be the most diverse. They range from the virtual "free pass" granted ISP's under the Communications Decency Act of the United States, where the ISP has no liability for the transmission of defamatory content, and no obligation to monitor such content, [7] to the more strict liability regime of China where an ISP can be held liable for the dissemination of such messages.[8]

Liability paradigms for "public order" violations seem to reflect more closely domestic policies regarding free speech and political or religious dissent. They range from the fairly liberal policies of the United States, with its strong free speech guarantees,[9] to Saudi Arabia which strictly controls the sexual and religious content of websites.[10] In fact, one of the most interesting developments in this arena is the ability of countries to control such information through filtering and strict regulation of who qualifies as an authorized service provider.[11]

Liability paradigms for copyright violations may be the most consistent on an international basis. Although to a certain extent the willingness of a particular country to hold an ISP liable for the infringing acts of third parties appears to be influenced at least in part by the liability paradigm used for other content control matters, copyright paradigms seem to reflect a general balance between the private rights of content owners

---

[7] Communications Decency Act, 47 U.S.C. §230.

[8] *See, e.g.,* China's Internet Regulations, Article 15 (prohibiting the production, reproduction, release or dissemination of information that insults or slanders other people…")(available in English at http://www.chinepulse.com).

[9] *See, e.g., Yahoo Inc. v. La Ligue Contre le Racisme,* 169 F. Supp. 2d 1181 (ND Cal. 2000)(court declines to enforce order of French court regarding illegal offer of sale of Nazi paraphernalia over the internet on the grounds that such order violates the First Amendment).

[10] *See, e.g.,* Saudi Arabia Council of Ministers Resolution (prohibiting content which is "insulting [to] the Islamic religion or the Saudi laws and regulations)(*cited in* Jonathon Zittain et al, *Documentation of Internet Filtering in Saudi Arabia* (available in English at http://cyber.law.harvard.edu/filtering).

[11] *See, e.g.*, Jonathon Zittain et al, *Documentation of Internet Filtering in Saudi Arabia*; Jonathon Zittain et al, *Empirical Analysis of Internet Filtering in China* (both available at http://cyber.law.harvard.edu/filtering).

and the general desire of the government to foster the growth of the internet as a source of information.

Progressive Liability Exemptions

In its initial stages, most countries provided strict liability standards for internet service providers for any illegal content contained on the Net. Thus, for example, in the United States in *Playboy Enterprises Inc. v. Frena*,[12] the operator of a computer bulletin board service was held to be directly liable for the unauthorized uploading and downloading by third parties of copyrighted photos.

As the threat that future growth of the internet might be unduly curtailed if ISP's were held strictly liable for all content on the web became more apparent, scholars and courts began to consider differential liability standards based on the level of control or volition an ISP exercised over a given activity. Thus, voluntary acts, such as creating a website, should give rise to a greater potential for liability than involuntary acts, such as transmitting of unedited third party content. As demonstrated below, this distinction between volitional and non-volitional acts is largely reflected in emerging international standards regarding ISP liability for copyright protected content.

Given the growing threat of piracy, pornography and other illegal materials on the internet, it is doubtful that any absolute exemption, even for third party content, will be established internationally.

Telephone Company? Bookstore? Or Last Clear Chance to Stop the Pirates?

In its earliest stages, most copyright issues were limited to the problem of preventing end users from posting, without authorization, copyrighted works for downloading by third parties. With the development of P2P file sharing, those may well be "the good old days" for copyright owners. Today's largest challenge is in preventing the uncontrolled dissemination of copyrighted works between end users. Often the only points of attachment for legal liability are the provider of the software that facilitates such transfer, the internet service provider, and the end user.

Despite clear differences in their nature, in many internet developed countries, ISP's are beginning to be viewed as closer to telegraph and telephone operators, at least insofar as liability for non-volitional acts are concerned. Nevertheless, without putting too fine a point on it, experience with internet content control in many countries demonstrates that one of the best ways for controlling content is by limiting the number of ISP's who are licensed to operate, and by imposing strict liability on these ISP's for any illicit materials that are transmitted. Studies of internet content control in countries such as China, Saudi Arabia and Singapore demonstrate that such control can be effective.[13] Although other harms may be created, including a limitation in the number of companies who are willing to assume such potential liability and a subsequent

[12] 839 F. Supp. 1552 (M.D. Fla. 1993).
[13] *See, e.g.,* Internet filtering studies cited in notes 10 & 11 *supra*.

constriction of domestic internet growth, the allure of solving content problems by imposing strict liability on all ISP's remains a potent challenge.

Sources for ISP Liability

This paper focuses primarily on ISP liability for third party copyright infringements. I've chosen this limitation for the simple reason that I believe there is actually a fairly clear international standard that is slowly emerging in this area. But even though this paper focuses primarily on copyright liability, this does not mean that other areas of the law can be ignored with impunity. To the contrary, rules in a country about ISP liability for copyright infringement may be hidden in other areas of the law.

For example, while the Singapore Free Trade Agreement ("FTA")(discussed in greater detail below) requires that ISP's be granted safe harbors for certain involuntary acts, these safe harbors are *only* for copyright infringing materials.[14] Singapore's licensing regulations, however, continue to impose liability for posting of material that is "objectionable on the grounds of public interest, public morality, public order, etc." [15] Thus, although activity may qualify as a safe harbor under the copyright laws enacted to comply with the FTA, the ISP may still be liable under Singapore's regulatory scheme. When constructing procedures for ISP clients, a broader view of the issue is clearly the wiser choice.

In crafting this broader view, ISP liability standards may be contained in domestic copyright laws (such as the Digital Millennium Copyright Act[16]), in defamation, tort and obscenity laws (such as in the Communications Decency Act[17]) in specialized internet, telecommunications and cable laws (such as in Japan's recently created Provider Law[18]), in ISP Licensing Rules and Regulations (such as in Singapore[19]), and in local regulations on internet content. Thus, for example, in ascertaining ISP liability in Japan, in addition to considering Japan's newly enacted Provider Liability statute, local ordinances such as the Okayama Municipal Ordinance banning slanderous posts[20] must also be considered in creating operational policy guidelines to reduce liability exposure.

Rules of Thumb

Subject to the vagaries of domestic law, as a general matter, ISP's will usually be held liable for their voluntary acts. If the ISP creates a web page with objectionable material, no country I am aware of will give him a safe harbor. Similarly, ISP's who

[14] *See* Singapore FTA, Chapter 22.16.
[15] Available in English at http://sba.gov/sg/netrg/code.
[16] 17 U.S.C. § 511.
[17] 47 U.S.C. §230.
[18] A Law to Limit the Liability of Specified Telecommunications Service Providers and Permit the Disclosure of User Information (available in English at http://www.media.is.tohoku.ac.jp/~jsimmons/MedLit/ProviderResponsibilityLawTranslation.html).
[19] *See* note 15 *supra.*
[20] *See generally* Dax Hansen, *A Web of Rules: How the Internet is Affecting Japanese Content Liability, Privacy, and Consumer Protection Laws* (November 2002).

have actual knowledge of illegal content will be held liable even if the content was created by an unrelated third party. The definition of "actual knowledge" and the duty to monitor may vary, but the willingness to impose liability based on such knowledge remains consistent. Finally, people who obtain a direct financial benefit from the illegal content can also expect to be held liable.

Even in the absence of knowledge or direct control, when it comes to determining liability for content, some content is worse than others. If the third party content falls into certain "danger zones," the likelihood of the ISP being held liable for such content increases dramatically. Thus, for example in Australia ISP's will be liable for material found to be "unsuitable for minors." [21] In Singapore, material which is "objectionable on the grounds of … public order or … national harmony" poses special dangers of liability.[22] Similarly in China, material which "endangers national security or …disturbs social order" falls within a danger zone where safe harbors are hard to find.[23] Generally speaking, content which is considered obscene, pornographic, harmful to minors, dangerous to the public order or which qualifies as hate speech is often excluded from any other safe harbors that might otherwise exist for third party content. Consequently, even if you find a jurisdiction that allows a safe harbor for some infringing speech, these types of content almost guarantee liability.

International Standards

Although both the WIPO Copyright Treaty and the WIPO Performances and Phonograms Treaty address copyright and neighboring rights issues on the internet, neither of them directly addresses the issue of ISP liability. Given the heated disputes over such fundamental issues as what right is impacted by unauthorized transmission of copyrighted material on the internet (Is it a distribution? A reproduction? A communication to the public?),[24] it isn't surprising that the more complex issues of ISP liability weren't directly addressed in the final treaty.

The lack of an international treaty on this issue, however, does not mean that international standards regarding ISP liability for third party material are wholly lacking. To the contrary, two different sets of documents have gone a long way toward establishing a growing international standard for ISP liability for third party content.

The first critical set of standards is found in the various European Union Directives governing the issue. The E-Commerce Directive[25] and the Copyright in the

[21] Censorship Acts, http://libertus.net/censor.
[22] *See* note 15 *supra*.
[23] China's Internet Regulations, Article 15 (available in English at http://www.chinaepulse.com)
[24] Mihaly Ficsor, *The Law of Copyright and the Internet* (Oxford 2002)(discussing the debates over such rights during the diplomatic conferences that led to the WIPO Copyright Treaty and the WIPO Performances and Phonograms Treaty).
[25] Directive on Certain Legal Aspects of Information Society Services, in particular Electronic Commerce (8 June 2000)(hereinafter "E-Commerce Directive").

Information Society Directive[26] have formed the basis, not merely for the domestic law standards for all current and future member countries of the EU,[27] but also for other countries who have just begun to deal with the issue.

The second set of critical standards is found in the free trade agreements between the United States and various trading partners, including Singapore, Australia, Bahrain, Morocco, and certain Central American countries.[28] The agreements ISP standards modeled strongly on the Digital Millennium Copyright Act of the United States.

On their surface, both EU and FTA standards have numerous features in common. Both acknowledge that ISP's deserve special consideration for their unique functions in serving as the transmission backbone of the internet. Both grant safe harbors to ISP's for certain non-volitional activities including transmission and storage so long as the ISP's serve no other role in the promulgation/distribution of infringing materials and earn no direct financial benefit from such infringing activities. Finally, both rely on a combination of notice and removal requirements to assist copyright owners in enforcing their rights on the internet. "The devil is in the details," however, and in this case those details can be problematic indeed.

The European Union Directives

Looking at the European Union Directives as a whole, they establish that certain non-volitional acts may qualify for safe harbor treatment where the ISP is involved in such non-voluntary acts as serving as a conduit for other's content,[29] caching, [30] and hosting (or storing)[31] third party material. To qualify for such harbors, the ISP must generally not modify the content at issue, must not select the recipients for the materials, and must not have any actual knowledge or "awareness" of the illegal content. Notably, and in contrast to the FTA standards discussed below, linking activities are not expressly mentioned as a safe harbor activity.

The "good news" for ISP's is that the safe harbor activities detailed in the European Union Directives are not limited to material which violates copyright laws. To the contrary, such safe harbors are potentially available for all content violations, including for example, defamatory or tortious speech.[32] In addition, the Directives do not impose an express duty on the ISP to monitor third party content.

---

[26] Directive on the Harmonization of Certain Aspects of Copyright and Related Rights in the Information Society (22 May 2001) (hereinafter "Copyright in the Information Society Directive).

[27] Whose number has increased with the recent expansion to 25 countries.

[28] The original signatories of the Central American Free Trade Agreement were Nicaragua, Costa Rica, Honduras, El Salvador, and Guatemala. Recently, the Dominican Republic has sought to have the FTA extended to it as well.

[29] E-Commerce Directive, Article 12.

[30] E-Commerce Directive, Article 13.

[31] E-Commerce Directive, Article 14.

[32] Since the Directives, however, are not generally self-executing, the extent of such safe harbors may differ under each country's domestic laws.

The "bad news" for ISP's is that the precise scope of activities which may give rise to "knowledge" or "awareness" sufficient to lose any safe harbor is not clearly set forth in the Directives. It will, necessarily, be subject to the vagaries of domestic law. Thus, for example, Recital 44 of the E-Commerce Directive, implemented by the E-Commerce Regulations in the United Kingdom states that a provider who "deliberately collaborates with recipients of a service to undertake illegal acts goes beyond the activities of a 'mere conduit'." The precise types of activities, however, that qualify as "deliberate collaboration" remain undefined.

Under the copyright laws of many countries "authorization" of an illegal act is itself considered an act of direct infringement. Thus, ISP's who "authorize" copyright infringing activities do not qualify as "mere conduits" because they are not simply providing transmission services. They are actually "authorizing" the illegal content. The line between transmission and authorization, however, has not yet been clearly delineated.

In the United Kingdom it takes an act beyond simply providing the means for the infringement to qualify as "authorization." In *Sony Music Entertainment (UK) Ltd v. Easinternetcafe Ltd,*[33] the court held the operators of an internet café liable for assisting patrons in downloading illegal files. The source of the liability was not the mere provision of internet access, but providing file copying facilities. Defendant's purported lack of knowledge of the infringing nature of the patron's files did not alter their potential liability.

Probably the clearest definition of what qualifies as authorization occurred in *Amstrad II* [*CBS Songs Ltd v. Amstrad*][34] where the court stressed that merely facilitating an infringing act is not sufficient. Instead authorization was defined as "to grant or purport to grant expressly or by implication the right to do the thing complained of..." The definition has yet to be applied in an ISP setting.

Similarly, in Australia, in another non-ISP case, *Moorhouse v. University of New South Wales,*[35] the court held that authorization occurred if the party failed to take reasonable steps to limit uses to legitimate purposes. Once again the mere provision of facilities is not sufficient. Instead some measure of control is required. Section 36 (1A) of the Copyright Act, as amended by the Digital Agenda Act of 2000, provides three factors that must be considered in determining whether authorization has occurred. These factors include the extent to which the person has the power to prevent the act in question, the nature of the relationship between the acting party and the authorizing party and whether the person "took any reasonable steps to prevent or avoid the doing of the act, including whether the person complied with any relevant industry codes of practice."

The "bad news" for copyright owners under the EU Directives is that they do not specify compliance with notice and take-down procedures for ISP's to qualify for safe

[33] 2003 WL 116984 (Chancery 2003).
[34] 1988 AC 1013 (1988).
[35] [1976] RPC 151 (High Court).

harbor treatment (unlike the DMCA and various FTA provisions discussed below). They do, however, require that at least in the case of caching and hosting (storing) activities the ISP must act "expeditiously" (for caching) [36] or "in due diligence" (for hosting)[37] to remove illegal material or disable access upon knowledge of its illegal content.

The EU Directives also do not provide any simplified subpoena measures for copyright owners to obtain subscriber identification information. In fact, obtaining such information may be particularly problematic in light of strong EU privacy protections contained in the EU Data Protection Directive.[38] This Directive, which provides strong limitations on the use of third party personal data, has not yet been interpreted to prevent the disclosure of subscriber identities. However, its stringent protection standards make it unlikely that any ISP in the EU would provide such information, absent a court order.

Court orders for the disclosure of subscriber information may require a relatively high level of proof of potential infringement. In *Ashworth Hospital Authority v. MGN Ltd*, [39] involving the identification of a journalist's source, the court granted the request for disclosure on the grounds that there was an "overwhelming likelihood" that a specific wrongdoing has been committed. This standard seems somewhat higher than the traditional prima facie evidence requirement. Moreover, in another UK case, *Totalise plc v. Motley Fool Ltd, [40]* dealing with the disclosure of the identity of an alleged defamer on the internet, the court indicated that the party seeking the disclosure should be required to pay the costs since any voluntary disclosure would be a breach of the Data Protection Act of 1998. Thus, while identification disclosures are available (and in fact have been used to combat music piracy), some countries may impose slightly higher costs for obtaining such information.

Free Trade Agreements

The United States has entered into a relatively large number of bilateral and regional free trade agreements in recent years.[41] From the point of view of developing international liability standards, since the Singapore Free Trade Agreement in 2003, each free trade agreement has contained virtually identical sections on ISP liability.[42] These sections, which first appeared in Chapter 16.22 of the Singapore FTA, basically establish the contours of the Digital Millennium Copyright Act of the United States (DMCA) as a new global standard for ISP liability.

---

[36] E-Commerce Directive, Article 13.
[37] E-Commerce Directive, Article 14.
[38] Directive Concerning the Processing of Personal Data and the Protection of Privacy in the Telecommunications Sector 15 (December 1997).
[39] 2002 WL 1310757 (House of Lords 2002).
[40] 2001 WL 1479825 (Court of Appeal 2001).
[41] Currently, FTA's have either been established or are in the negotiating stages for the following countries: Andean Community (Columbia, Peru, Ecuador, Bolivia); Australia; Bahrain; CAFTA (Costa Rica, El Salvador, Guatemala, Honduras, Nicaragua); Chile; Morroco; Singapore; and South African Customs Union (Botswana, Lesotho, Namibia, South Africa, Swaziland).
[42] This observation is based on a review of the ratified drafts of the FTA and on the proposed official drafts of the FTA's that have not yet been ratified. These drafts can be found the on USTR's website under http://www.ustr.gov/fta.

Under Chapter 16.22 four non-volitional activities by ISP's qualify for safe harbor treatment. They are: serving as a conduit for third party content,[43] storing (hosting) such content,[44] caching,[45] and linking.[46] To qualify for such safe harbors, ISP's must generally not initiate the transmission. They cannot select the recipients or modify the material in question. For certain activities, the ISP's must also comply with notice and takedown requirements,[47] and must not receive any direct financial benefit from the hosting or linking of the material at issue.

The "good news" for ISP's is that the FTA's, similar to the EU Directives, do not impose an express obligation on ISP's to monitor third party content.

The "good news" for copyright owners is that the FTA's also impose notice and take down procedures that largely mirror those in the DMCA. For those ISP's engaged in storing (hosting) or linking activities, Chapter 22.16(ix) of the Singapore FTA requires countries to establish "appropriate procedures for effective notifications of claimed infringement, and effective counter-notifications by those who material is removed or disabled through mistake or misidentification." Chapter 22.16(x) further provides immunity for ISP's who remove or disable access to material "in good faith" so long as they take "reasonable steps promptly to notify" the person making the information available and comply with counter-notification procedures. In addition, a representative to receive such notifications must be "publicly designated."[48] The precise content of the notices is not specified in the treaty. However, they must be "effective," which would appear to require fairly specific information about the identity of the material in question, and its location. Receipt of such a notice is a "circumstance" from which the infringement is "apparent."[49]

The FTA's further require each country to establish "legal incentives for service providers to cooperate with copyright owners in deterring the unauthorized storage and transmission of copyrighted materials." The precise nature of those incentives is not specified. However, such language would seem to indicate that, within such the safe harbor exemptions specified in the agreement, domestic policy must still require that some share of the burden for reducing piracy remain with ISP's.

Finally, the FTA's require administrative or judicial procedures that enable copyright owners to obtain "expeditious" disclosure of end user "information."[50] To qualify for such disclosure the copyright owner must have previously given "effective

[43] Singapore FTA, Chapter 22.16 (A).
[44] Singapore FTA, Chapter 22.16(C).
[45] Singapore FTA, Chapter 22.16(B).
[46] Singapore FTA, Chapter 22.16(D).
[47] These activities include hosting and linking. Caching also requires take down but only upon notice that the original materials have been removed or access has been disabled at the originating site. *See generally* Singapore FTA, Chapter 22.16 (iv).
[48] Singapore FTA, Chapter 22.16(v)(C).
[49] Singapore FTA, Chapter 22.16(v)(B).
[50] Singapore FTA, Chapter 22.16(xi).

notification of claimed infringement." The "information" must be in the "possession" of the ISP and must "identify" the alleged infringer. There is no affirmative obligation to recreate end user information.

The "bad news" for ISP's is that, unlike the EU Directives, the FTA's limit the granted safe harbors to copyright and related rights infringements. The "bad news" for copyright owners is the lack of clarity regarding who is required to provide expeditious identification information. Similar to the DMCA, the language regarding the duty to disclose end user information is tied to the provision of "effective notice" of infringement. Under the language of Chapter 22.16, safe harbor acts of storage (hosting) and linking are specifically premised on the expeditious removal or disabling access on actual knowledge or awareness of infringement, including "effective notice."[51] The act of caching similarly requires expeditious removal or disabling access on receipt of effective notification.[52] Conduit activities impose no such obligation. Yet the obligation to establish administrative or judicial proceedings to require the disclosure of end user identification is tied to the receipt of "effective notification of claimed infringement."

This failure to require conduit ISP's to comply with removal notifications in the DMCA led the DC Circuit Court of Appeals to refuse to apply the expedited subpoena process of Section 512(h) to conduit ISP's. [53] Although treaty language is not generally the same as a statute, and is not subject to the same rules of interpretation, there is a strong likelihood that this lack of clarity might be relied upon to avoid requiring identity disclosures based solely on conduit activity.

Selected Issues under National Standards

While there are emerging international standards regarding ISP liability, national standards still play an important role in determining the contours of ISP liability. The following contains a brief discussion of some of the more interesting domestic variances in ISP liability for third party content.

Notice and Take Down

Many countries acknowledge that ISP's should be obligated to act to remove or disable access to infringing material when they have notice of the infringing nature of such materials. Countries, however, may differ on the nature of the obligation imposed, or the quality of the notice required. Thus, for example, in Japan under its Provider Liability Law, the ISP has an affirmative obligation to convey information to the end user of any notice and to prevent the transmission of such material if the end user does not object, *and* if it has technological ability to do so. The ISP, however, is given a certain

[51] Singapore FTA, Chapter 22.16 (v)(B).
[52] Singapore FTA, Chapter 22.16(iv)(D).
[53] *See RIAA v. Verizon Internet Services*, 351 F.3d 1229 (DC Cir 2003).

amount of flexibility to take action based on its own assessment of the alleged infringement.[54]

In China, failure to remove infringing content where the ISP has obtained "clear knowledge" or is warned by the copyright owner "based on solid evidence" of the infringement results in joint liability with the end user.[55] The type of evidence which qualifies as "solid evidence" is not specified in the Guidelines or in China's Internet Regulations.[56] However, it would appear that at least a prima demonstration of infringement may be required for an effective notice to require take down of the allegedly infringing material.

Subpoena for End User Identities

In addition to the difficulties posed in those countries which follow EU standards on personal data privacy, several countries have recently demonstrated a more critical view toward granting disclosure orders connected with internet piracy complaints. Perhaps the most significant decision in this arena is the recent Canadian decision in *BMG Canada v. John Doe.*,[57] In this case diverse recording companies sought an order to obtain the identity of end users who were allegedly involved in illegal P2P file trading of infringing music. The court denied the request for identity disclosure. Emphasizing the strong privacy concerns at issue, the court ultimately found that the use of what have become "standard" affidavits attesting to the presence of unauthorized files on a computer at a particular internet protocol address was insufficient to warrant the order. To a large extent the case turned on the specifics of Canadian domestic law which expressly provides that downloading a song for personal use does not qualify as an infringement. The court's comments however were not so limited. At its heart, *MBG Canada* demonstrates a rejection of pro forma identity disclosure requests, at least in connection with music piracy, and applies a stringent, and somewhat skeptical, evidentiary standard for demonstrating sufficient infringement, including requiring of causal link between P2P pseudonyms and IP addresses. The case is currently on appeal.

The Fair Use Exception

Obviously ISP's can only be held liable if the content at issue is actually infringing. Many countries, such as Canada, recognize some form of personal use right for music. Thus, unauthorized downloads may not qualify as infringing activity. (Distribution or making available such copies to others, however, may qualify as infringing activity.) One of the most comprehensive lists of fair use activity which may be considered in determining IPS liability is contained the EU Copyright in the Information Society Directive. Article 5(3) contains a detailed list of potential fair uses

[54] *See generally* J. Dax Hensen et al, *Japan, Inc.: A Web of Rules: How the Internet is Affecting Japanese Content Liability, Privacy and Consumer Protection Laws* (November 2002).
[55] Supreme Court Guidelines on ISP Liability, Article 5.
[56] These are available at the website http://www.chinaepluse.com
[57] 2004 FC 488 (Ottawa 2004).

that can be granted for the rights of reproduction, communication and making available. They include the following:

1) For teaching or scientific research:
2) For the benefit of people with a disability;
3) For news reporting purposes;
4) Quotations for criticism or review;
5) For the purposes of public security or "to ensure proper performance of reporting of administrative, parliamentary or judicial proceedings;"
6) For Informatory purposes if the work is a political speech or public lecture;
7) For use during religious celebrations or official celebrations organized by a public authority;
8) Use of works of architecture or sculpture located permanently in public places;
9) For advertising artistic works for sale;
10) For caricature, parody or pastiche;
11) In connection with demonstration or repair of equipment;
12) For reconstructing a building;
13) For research or private study on dedicated terminals.

All such exceptions are subject to the tri-partite test that they only be applied "[1] in certain special cases [2] which do not conflict with a normal exploitation of the work or other subject matter and [3] do not unreasonably prejudice the legitimate interests of the right holder." [58]

Some Practical Tips for Reducing ISP Liability Internationally

In order to reduce potential liability, the following considerations and procedures appear to be in keeping with emerging international trends for reducing ISP liability:

<u>General Rules for Limiting Liability</u>

- Don't initiate transmissions, edit content or control recipients

- No "authorization" for illegal activities, including avoiding posting advertisements on file sharing sites[59]

- No tutorials showing use of the service to accomplish illegal acts (such as "how to" instructions for using a service which features how to download illegal music)

[58] EU Directive on Copyright in the Information Society, Article 5(5). This language mirrors the fair use language of TRIPS, Article 13.
[59] Such activity may cross the line between merely serving as a conduit, and actually authorizing illegal P2P file trading in those countries where "authorization" is a separate activity.

- Establish procedures for responding to notices from copyright owners. These should include:
    - Public identification of the address/person designated to receive notices
    - A checklist to be certain that received copyright notices establish all the information necessary to establish a prima facie case of copyright infringement
    - Notices to end users of intent to remove allegedly infringing material
    - Prompt removal or disabling of access of such material
- Maintain Accurate Records of End User Identities
- Release End User Identity Information Only Upon Appropriate Court Order
- Maintain Right to Terminate Services Upon Misidentification of End User

While these procedures should help ISP's qualify for safe harbor exemptions under emerging international standards for their non-volitional acts, the precise contours of such procedures should be formulated with an eye to domestic variations as well.

The Future

Despite the many vagaries concerning ISP liability that remain internationally, there is little doubt that de facto international standards are slowly emerging. While these standards remain in flux, it appears that there is a growing trend to hold ISP's exempt from liability for carrying third party content over which they exercise no control. These trends should continue. However, the duty of the ISP to assist the copyright owner to remove or disable access to infringing content, I believe, will continue to be strengthened internationally. Those ISP's who receive notices of potentially illegal third party content will remain at peril.