PART II: Filtering the Internet to Prevent Copyright Infringement: ISP Safe Harbors and Secondary Liability in the U.S. and France

INTRODUCTION

Part I of this article provided a background and an overview of the principal international treaties and European Union ("EU") directives related to copyright infringement on the Internet and safe harbors against such liability for Internet Service Providers ("ISPs"). Part I also presented a summary of the Digital Millennium Copyright Act ("DMCA"), which was implemented to effectuate these treaties, and the law of ISP secondary liability in the U.S. This Part II presents an overview of French national law and judicial decisions on the same subject. Part I noted that fairly recent advances in technology, in particular the development of Deep Packet Inspection ("DPI"), make monitoring and filtering of content transmitted over the Internet that disables access to copyright infringing materials increasingly feasible and practicable. Part II focuses on recent enactments and judicial decisions in France and some other EU Member Nations which implicate an ISP obligation to monitor and filter (or "screen") the Internet to prevent copyright infringements. It compares French and U.S. law and legal developments in this area and provides a brief overall assessment of the legal implications of Internet filtering technology for ISPs and copyright owners.

William C. Harrelson
Tobin Law Group PC

SECONDARY LIABILITY AND SAFE HARBORS IN FRANCE

As noted in Part I, the EU's E-Commerce Directive ("ECD") establishes ISP safe harbors very similar to the DMCA safe harbors in the U.S. The ECD, however, is broader in coverage. It provides "horizontal immunity" not just for copyright infringement, but for other forms of liability related to information ISPs make available on the Internet, such as defamation, misleading advertising, or trademark infringement. In France, the ECD was implemented into national law in 2004 in the Law for Confidence in the Digital Economy ("DEL"),[1] which closely follows the safe harbor provisions of the ECD. Initially, ISPs expressed extreme displeasure over the bill. One French ISP group described it as "an incoherent hodgepodge which even internet professionals are hard put to understand."[2] As is the case with the DMCA and common law in the U.S., while the ECD and DEL define certain limits for the application of direct, contributory or vicarious liability to ISPs, they do not eliminate the risk of liability. Even though copyright law as codified in France does not have specific provisions that address contributory or vicarious liability, the French civil and penal codes, like U.S. common law, recognize basic legal principles that can apply to impose secondary liability on ISPs.[3]

French Decisions Prior to the Digital Economy Law

French courts tended to insulate ISPs that were "mere conduits" from copyright liability even prior to France's implementation of the ECD's safe harbor provisions. Consistent with *Perfect 10* in the U.S., French decisions held that an ISP providing links to other possibly infringing websites alone will not give rise to liability,[4] reflecting that linking or interconnection is an intrinsic and desirable characteristic of the Internet. On the other hand, actual hosting by an ISP or display by a website, even though at the instance of a user, could give rise to secondary liability. The law in France on this point was unclear, with the courts requiring prudence, cautiousness ('*diligences appropiees*') and sometimes screening to detect and disable "obviously" illicit activity.[5] In 2000, the Cour d'Appel of Versailles reversed a lower court decision holding an ISP liable on the basis that it should have used a search engine to find key words that would detect an infringement and then notified the author or disabled the apparently infringing website. The appellate court rejected a systematic monitoring requirement. It instead imposed a standard akin to the *Netcom* approach in the U.S. Thus, prior to enactment of the DEL in France, a court rejected a systematic monitoring requirement and found that disabling access should only be required as to specific content where the ISP had "actual knowledge or is informed of the illicit content of a website or when the ISP comes to suspect illegality of content while performing its ordinary tasks on the website at stake."[6]

On the other hand, the often commented upon *Yahoo!* case illustrates a French courts' willingness, before the DEL was en-

acted, to require the use of filtering technology to screen offending content. It shows French courts are not reticent to exercise jurisdiction and their broad injunctive power over Internet operations based in other nations to the extent there is some cognizable harm within their borders. The *Yahoo!* case involved Yahoo!'s encounter with French penal laws barring the display of Nazi paraphernalia. It illustrates the clash the seamless worldwide reach of the Internet created between two cultures placing different emphasis on protection of speech—the U.S. cherishing utmost free speech and France restricting speech seen as possibly promoting Nazism. In 2000, a French court required Yahoo! to implement screening and filtering technology to "take all measures to dissuade and make impossible any access by a surfer calling from France" through Yahoo.com to the sites and services displaying Nazi paraphernalia. If it disobeyed, Yahoo! was confronted not only with stiff monetary fines, but its executives were also threatened with imprisonment. Yahoo! insisted that the measures ordered were technically impossible because the nature of the Internet left it unable to deny access to French citizens without simultaneously denying access to Americans. Losing in the French courts, Yahoo! resorted to its home jurisdiction and sought an order in the U.S. declaring the French order unenforceable because it was repugnant to the 1st Amendment. Ultimately, a divided Ninth Circuit dismissed the case on grounds it was not ripe and for lack of personal jurisdiction without reaching the merits.[7]

The French Digital Economy Law

Article 6 of the DEL addresses liability of ISPs, known in Europe as providers of "information society services." Like the ECD, the DEL takes a horizontal approach, addressing not only copyright infringement but all forms of civil and criminal liability related to online content. Article 6 provides that a host provider may incur liability, if: 1) it was aware of the unlawful nature or facts and circumstances pointing to the unlawful nature of information posted by its users; and 2) does not take prompt action to withdraw or disable access to the data. The ISP is deemed to be aware of the unlawful nature of content if it has been sent notification in accordance with the specified procedure and form.[8]

Since its passage, French courts have most often applied Article 6 to restrict copyright liability of ISPs to circumstances where the ISP had "actual knowledge" of "obviously illicit" content or failed to promptly take down information after actual notice. In the first decision dealing with an ISP's responsibility for content under the law, a Paris court was presented with the question of whether the content posted by the ISP was "manifestly illegal." The question was legally complex, involving analysis of several French national laws and international treaties to determine if the posted content unlawfully provided justification for war crimes. The Court held the ISP was not liable under the "manifestly illegal" standard.[9] In a 2007 defamation and invasion of privacy case, a French court applied Article 6 to find that eBay Europe and eBay France were hosting providers having no "general obligation to monitor the information stored, or to search for facts or circumstances indicating illegal activity."[10] As to the requisite level of knowledge, the Court of Appeal for Versailles has ruled that, if knowledge is based on notice or complaint by one alleging illicit activity, an ISP is entitled to "precision as for the facts complained of and their site [*i.e.,* location]."[11] While these cases deal with claims other than copyright infringement, they nevertheless indicate how French courts implement the ISP safe harbors in the DEL, since the DEL applies safe harbors not only to copyright infringement but also to other causes of action based on information ISPs make accessible on the Internet.

Publisher Liability and Filtering

French courts have issued inconsistent decisions on the issue of whether a website merely hosts or takes on the role of a publisher or editor. If a website is found to be a publisher, it is not entitled to the hosting safe harbor in the DEL and can be found liable for damages for content posted on its website. Under French law, publishers are primarily liable for a "litigious message."[12] The DEL extended the liability regime applicable to the press in the area of privacy violations to "persons engaged in the business of publishing online communication services."[13] Cases involving defamation or common law privacy actions in the U.S. would fall under the provisions of the Communications Decency Act (CDA"), rather than the safe harbor provisions of the Copyright Act. The CDA basically provides that no ISP (provider of an interactive computer service) can be treated as a publisher or speaker of information that another person or entity is responsible for creating or developing.[14] The immunity is very broad and would insulate an ISP from liability in the U.S. for content created by third-parties, such as the ISP's users. An ISP remains liable, however, for any illegal content that they create or "cause" to be created.[15] At the same time, an ISP will not be held liable under the CDA for actions it takes to restrict access to "objectionable" material, even if it is constitutionally protected.[16]

One trend on the Internet is the growth of diverse multimedia interactive websites known as "Web 2.0" sites. These include social networking sites (MySpace, Facebook and LinkedIn), peer-to-peer file sharing technologies (such as the former Grokster and now BitTorrent), user generated content platforms (YouTube, the former Google Video, MySpace, Facebook and Wikipedia), virtual worlds and online games (Second Life, Guild Wars, City of Heroes), and various kinds of blogs. The increasing complexity of the role of Web 2.0 sites has made it difficult for the French courts to draw a bright line between an ISP that is merely a host and one that acts as a publisher. In a recent French case, a Web 2.0 site in France called Fuzz.fr was held liable for breach of privacy and ordered to pay damages as a

publisher for linking to a separate website containing gossip about the love life of a French actor. In concluding that Fuzz.fr was a publisher, the court relied on a finding that it made "editorial decision[s]." In particular, Fuzz.fr placed links on its website to another site that contained gossip about the French actor and determined "the organization and presentation of [its own] site," including posting a title that referred to the actor's private life. As a whole, this activity was held to be an act of publication with "the intent to put the general public in contact with messages of [Fuzz.fr's] choice." The decision is consistent with a line of prior decisions, which applied the publisher status to any ISP that: 1) "organizes a hosting structure to publish stored information," and 2) financially gains from sponsoring Web 2.0 sites through advertising revenues.[17]

A second line of French cases, however, finds similar Web 2.0 sites not liable as mere hosting ISPs. The distinguishing factor is the finding that the ISP did not initiate the dissemination of the hosted content, which the courts' found to be the essential role of a publisher. In these cases, the courts rejected financial gain from advertising and control over the organization of the websites as determinative. This line of reasoning has been used by French courts in cases holding under the circumstances presented that Wikipedia,[18] a chat forum,[19] and eBay[20] were host providers entitled to safe harbor. In a recent decision, a Paris court held that YouTube qualified as a host provider and was not a publisher of its end users' postings. The court noted the DEL defines a hosting provider as "the person who makes available to the public online communications services, storage services" of information of any kind "supplied by end users of the services." The Court also supplied a definition of website publisher as "the person who determines the contents made available to the public from the service it created or is in charge of."[21]

The owner of Fuzz.fr has appealed the Fuzz.fr decision, on the basis of this second line of decisions, emphasizing Fuzz.fr's passive role—its use of automated classification tools for organization of user content on its website and lack of control over the content itself.[22]

In a recent 2007 decision, the court classified MySpace as a publisher and disqualified it for safe harbor under the DEL. The case upheld the claim of a French humorist against MySpace for infringement of his author's and personality rights, after several of his skits were posted by a user on one of the site's webpages. Despite the fact that MySpace performed the function of a "hosting" service (arguably entitled to the immunity of Article 14 of the ECD as implemented in Article 6.I.2 of the DEL), the court disqualified it because MySpace imposed a "pre-designed page setup for users' personal accounts" and exhibited "revenue-generating advertisements…upon each visit."[23] A recent paper, "Filtering the Internet for Content in Europe" published by the European Audiovisual Observatory, points to this decision as encouraging websites to use automatic filtering systems to avoid the posting of infringing material. The paper examines whether filtering of the Internet to protect copyright is consistent with the European legal framework. It concludes "the provisions of the E-Commerce directive lead to conflicting interpretations."[24]

Injunctive Relief and Filtering

French courts have recently struggled to reconcile the availability of Deep Packet Inspection and sophisticated filtering tools with the apparent ban on the imposition of a general monitoring obligation in Article 15 of the ECD. The ECD requires European Member Nations to provide safe harbors from monetary relief but it does not clearly limit the broad injunctive powers of EU national courts. There is an argument that because the ECD limits the imposition of a monitoring requirement to only "in a 'specific case' (Recital 47)" an injunction ordering monitoring is appropriate only when "specific people, websites or content are affected." On the other hand, the ECD only immunizes ISPs from monetary damages and each of the safe harbors in Articles 12 through 14 provides that "courts and administrative authorities" may "terminate or prevent an infringement." Also, Article 8(3) of the ISD specifically instructs Member Nations to make provisions allowing rightsholders to obtain injunctions against infringements and Article 9(1) of the ECD reinforces this right.[25]

On May 6, 2009, the Paris Court of Appeal overruled a controversial lower court decision holding a videosharing website liable in the *Dailymotion* case. The lower court ruled that despite Dailymotion's advertising-based business model, it was a host provider not a publisher. Nevertheless, reminiscent of *Napster,* the lower court held the requirement for actual or apparent knowledge of specific infringements did not apply where the unlawful activities were generated or induced by the host provider. The lower court held Dailymotion liable for damages for not implementing technical filtering measures to monitor and disable infringing activities. The appellate court reversed, finding Dailymotion was not liable because it had not received adequate notification that the copyrighted film posted to its website was infringing and because rights holders had not complied with the DEL's requirement that notifications indicate precisely which content is alleged to be unlawful, why it is unlawful and its precise location on the website.[26]

In late-2008, however, another lower court ruled that once Google Video was notified of infringing content, it must not only remove the content but take measures to ensure that particular content is not reposted. Each time the infringing film reappeared on Google Video's website, the owner sent formal notice demanding removal, and each time Google Video complied. Nevertheless, the Court held that Google Video was obligated to take all steps necessary, including monitoring and filtering, to prevent further publication of the film.[27] Some commentators express the view that the *Google Video* ruling has broad implica-

tions, allowing in effect a court to impose a general monitoring and filtering obligation. The ruling certainly required monitoring and screening by Google Video to prevent re-postings of the particular infringing film to avoid liability. But also, as single notices of infringement accumulate with respect to numerous works, the only practical way for an ISP to comply with the *Google Video* rule is to employ automatic filtering technology.[28]

RECENT DECISIONS IN OTHER EUROPEAN NATIONS

A recent landmark decision in Belgium combats Internet copyright piracy on a website facilitating peer-to-peer file sharing by issuing an injunction imposing filtering obligations on the underlying Internet access providers or IAPs. This decision extends "gatekeeper" responsibilities deep into the Internet, below the level of a website or even a host provider, down to the underlying provider of Internet access. In the *SABAM* case, the Belgian Society of Authors, Composers and Publishers ("SABAM") alleged a Belgian IAP knowingly permitted the infringement of its members' protected works through the downloading of files and the using of peer-to-peer file sharing on its networks. SABAM sought an injunction and the court, after enlisting the report of its own technical expert, ordered the IAP to employ specific Internet filtering technology to prevent further downloading of SABAM copyrighted music using filesharing software. The court rejected the argument that the relief was contrary to the ECD's proscription of a general obligation to monitor. It partly relied on Recital 40 of the ECD, which generally provides that its limitations on liability "should not preclude the development and effective operation of technical systems of protection and identification." The court also concluded there was no general monitoring obligation, since the filtering instruments would block only certain, specific information. The IAP has appealed the decision.[29] The favorable reaction of international rightsholder groups to the decision is represented by the press release of the International Federation of Phonographic Industries, announcing "this is an extremely significant ruling which bears out exactly what we have been saying for the last two years—that the Internet's gatekeepers, the ISPs, have a responsibility to help control copyright-infringing traffic on their networks… and the technical means to tackle piracy."[30]

In the *Pirate Bay* case, an appellate court in Denmark upheld a lower court decision ordering an IAP to block access to the Swedish Pirate Bay website, which facilitates peer-to peer file sharing using BitTorrent. The holding was that the ECD shields only against damages, not injunctive relief under Denmark's national law.[31] An Italian court, on the other hand, refused essentially the same relief against Pirate Bay. The court held under its national law that a personal injunction against an online intermediary outside of Italy is only permitted in specific cases; copyright infringement not among them. At bottom, these cases indicate that the issue of the permissible breadth of injunctions and whether they may impose monitoring and filtering obligations on an ISP or order an ISP to disable access to a website is one governed by the national laws of the individual European nations.[32]

While this article was being drafted, a court in Milan, Italy sentenced four Google executives to six months in jail and ordered them to pay fines for violating a young man's right to privacy. A user posted a clip on Google Video showing a boy with Downs' syndrome being harassed by teenagers. According to reports, Google removed the video within hours of being notified by the Italian police but about two months after it had been posted and some users had already complained that it should be removed. Google was found negligent for not doing enough to keep the offensive video off its site.[33] Prosecutors argued Google management was responsible for the content because of its advertising-based business model.[34] The case appears to follow the seriously questionable line of divided French cases represented by the Fuzz.fr decision discussed above. These cases find publisher liability where the site organizes a hosting structure and financially gains through advertising revenues, even though the ISP is not responsible for posting, creation, or development of the content. Google's statement noted: "European Union law was drafted specifically to give hosting providers a safe harbour from liability so long as they remove illegal content once they are notified of its existence."[35] Google also asserted that "screening or editing the contents of user-generated video sites in advance is impossible because of the volume of material that is posted."[36]

THE FRENCH DIGITAL PIRACY LAW

In late 2009, a new French law to combat digital piracy, nicknamed the "three strikes law," became effective after withstanding the scrutiny of France's highest constitutional authority.[37] It creates a new state agency empowered to refer repeat offenders to a judge, who is able to cut-off a person's Internet access and impose substantial fines through a simplified process akin to that for a traffic violation.[38] Government sources estimate that 180,000 cases will be brought[39] and 50,000 sanctions will be levied annually under the law.[40] Over two-dozen judges will administer the penal system. A previous version of the law, which gave the agency the final power to order termination, was struck down by the high court after it ruled that Internet access is a "fundamental human right." Under the new version, only a court has the power to finally order termination. Based on a description of the previous initial accord reached in November of 2007 between the French government and rightsholder groups (generally the music and film industry), the law likely reflects "voluntary" monitoring by ISPs to police their networks.[41]

The film and music industries have not sought similar legislation in the U.S. But as in the case of the evolution of the DMCA, U.S. trade representatives could in effect agree to

implement a similar law through the Anti-Counterfeiting Trade Agreement ("ACTA") currently being negotiated between the United States, Japan, the European Union and other nations.[42] A very similar law has just been introduced in the British parliament.[43] France's "three strikes law" appears to be a very controversial political compromise between high stakeholders, the motion picture and recording industry and ISPs. ISP exposure to liability is reduced in return for cooperation to "voluntarily" monitor and "turn over" to authorities offending Internet users. The new law reflects either acknowledgement by the ISP industry or at least the French government's strong belief that comprehensive monitoring by ISPs is technically and practically feasible. The law could be viewed as precedent for requiring ISPs to implement filtering technology and, at a minimum, reflects legal and technical acceptance of comprehensive monitoring by ISPs. Interested parties should carefully follow negotiations surrounding the ACTA to see whether a treaty obligation similar to the French "three strikes law" becomes a part of the agenda.

INJUNCTIVE RELIEF AND FILTERING IN THE U.S.

Monitoring and Filtering Under the DMCA

The DMCA strictly limits the form of injunctive relief a U.S. court may fashion where an ISP qualifies for one of the safe harbors. Basically, for the caching and hosting safe harbors, a court may only restrain the ISP 1) "from providing access to infringing material or activity residing at a particular online site" or 2) by ordering termination of "specified" accounts of a subscriber or accountholder. A court may grant other injunctive relief only if considered necessary to restrain "infringement of copyrighted material specified in the order at a particular online location" and it is the least burdensome (to the ISP), comparably effective relief. The forms of injunctions permitted against "mere conduit" ISP functions are even more limited, being limited strictly to ordering: i) the equivalent of (2) above; or ii) the blocking of access to "a specific, identified, online location outside the United States."[44]

By its terms, Section 512(j) does not permit a court to issue an injunction in a form that imposes on an ISP an obligation to monitor and filter to prevent unspecified copyright infringement at unspecified online locations or by unspecified subscribers, so long as the ISP qualifies for one of the safe harbors. These limitations on the form of injunctions are consistent with the general "notice and takedown" scheme of the DMCA. DMCA Section 512(m) eschews any general monitoring obligation of ISPs, "except to the extent consistent with a standard technical measure." An ISP qualifying for the hosting or search tool safe harbor under the DMCA is entitled to notice that identifies with specificity the material claimed to be infringing and information sufficient to locate it. Similarly, injunctive relief against these ISP functions is essentially limited to ordering the disablement of access to specified material at specified locations or the termination of the accounts of specified repeat infringers. An ISP must, in fact, adopt and implement a policy for terminating the accounts of repeat infringers to qualify for safe harbors.[45]

The paper "Filtering the Internet for Content in Europe" suggests that an ISP filtering obligation could be accommodated under Section 512(m)'s provision making an exception for monitoring that complies with "standard technical measures."[46] But "standard technical measures" are defined as those "used by copyright owners to identify or protect copyrighted works" that, among other requirements, have developed into an industry standard pursuant to a consensus of copyright owners and ISPs.[47] Thus, while the employment of sophisticated filtering technology voluntarily by industry consensus between ISPs and copyright owners is permitted, the DMCA does not permit general monitoring and filtering to be judicially imposed, either by injunction or as a condition for escaping liability for damages.

Monitoring and Filtering To Prevent Contributory or Vicarious Infringement

On the other hand, a form of monitoring and filtering may be required as part of injunctive relief in cases of contributory or vicarious infringement. Part I provided an overview of the law of contributory and vicarious infringement in the U.S. The *Napster* case held that the DMCA does not necessarily shield an ISP that is found to be a contributory or vicarious infringer. The federal district court had concluded that the applicable DMCA safe harbor did not apply to protect Napster against contributory infringement as a matter of law because it "expressly excludes from protection any defendant who has '[a]ctual knowledge that the material or activity is infringing,'…or 'is aware of facts or circumstances from which infringing activity is apparent.'"[48] The 9th Circuit declined to adopt a *per se* rule that DMCA safe harbors will never apply in a case of contributory or vicarious liability. But it upheld a modified preliminary injunction requiring monitoring and filtering to prevent infringements, while leaving the ISP's ultimate qualification for a DMCA safe harbor as a fact issue for trial.[49] Suffice it to say that if the actual knowledge and material contribution elements of contributory infringement are met or an ISP can be found vicariously liable because it turned a blind eye to detectable acts of infringement for the sake of profit, an ISP will have a tough time convincing a court or jury that it qualifies for the hosting or information location tool safe harbors under the DMCA, certainly at least at the preliminary injunction phase. If the ISP does not qualify for a safe harbor, Section 512(j)'s limits on the form an injunction may take also do not apply. Even in such cases, however, an injunction may not place the entire burden of detecting and preventing infringements on the ISP. In *Napster*, the 9th Circuit modified the district court's original broadly worded injunction to require plaintiffs "to provide notice to Napster of copyrighted works and files containing such works available on the

Napster system before Napster has the duty to disable access to the offending content."[50] The final injunction upheld by the 9th Circuit required the ISP to affirmatively monitor and filter its system but only for initial and updated lists of the owner's specific copyrighted works found on one or more files available on the Napster system. The lists were to be supplied by the copyright owners.[51]

CONCLUSION

International law governing ISP safe harbors so far generally favors an opt-out model. A copyright owner must provide detailed notice of specific infringing material or activity and its location on the ISP network before an ISP can be liable for damages. The ECD and France's DEL, as well as the DMCA reject, consistent with an opt-out regime, any general monitoring or filtering obligation to prevent copyright infringement. An "opt-out" model may be viewed as inconsistent with the WCT's and WPPT's securing of a right of copyright owners to authorize communication to the public over the Internet. But the WCT expressly notes that merely providing facilities enabling a communication to occur is not a "communication" and the ECD explicitly provides that an ISP does not have an affirmative duty to monitor for offending content. Safe harbors, however, do not necessarily apply if the ISP engages in activity seen as knowingly inducing or contributing to infringement or turning a blind eye to and profiting from obvious infringement.

There is growing pressure on ISPs to use modern screening technology to monitor for or screen copyright infringement both for business reasons and by legal compulsion. Some legal experts in the field advocate imposition of gatekeeper responsibility on ISPs, arguing that modern filtering technology makes screening feasible and practicable and, in effect, makes ISPs the least cost avoiders of infringement or other illicit activity.[52] One expert represents the view that the law of copyright must be enforced by ISPs, or copyright as it is presently constituted will cease to exist. He acknowledges that current U.S. law presents formidable impediments to implementation of such a regime through judicial mandate and recommends cooperation between ISPs and copyright owners to accomplish this end.[53] Under the current state of the law, however, implementation of voluntary monitoring presents some risk that an ISP will lose safe harbors because it could be found to have "actual knowledge" or "red flags" of infringements as a result.[54] Moreover, automatically disabling access using filtering technology may expose an ISP to liability under the DMCA for blocking fair use of copyrighted works.[55]

Recent decisions in the EU show an increased willingness to grant injunctive relief requiring monitoring and filtering or to impose liability under circumstances which require, as a practical matter, monitoring and filtering to avoid liability. These cases generally fall into one of three categories. One category, represented by the French Fuzz.fr and MySpace cases, arises where a court finds the ISP engaged in an editorial or publishing role with respect to the offending content and, thus, not entitled to the hosting safe harbor. The second category, represented by the French *Google Video* case, imposes such relief only upon finding that the ISP did not act adequately to prevent repeat infringements of specifically identified protected works. A third category, represented by the Belgium *SABAM* case and the overturned French lower court ruling in the *Dailymotion* case, employs the relief in circumstances analogous to *Napster*, where a U.S. court might find the offending website liable for contributory or vicarious infringement.

Publisher Liability

Europe's greater willingness to order monitoring and filtering results in part from the horizontal approach to ISP immunity taken under the ECD. The issues involved in application of ECD safe harbors bleed over into enforcement of laws that may be viewed as protecting interests more fundamental than copyright, such as penal laws against the promotion of fascism or privacy rights seen as protecting human dignity. The greatest confusion and risk, particularly for interactive networking websites, is the European courts' inconsistent treatment of what activity gives rise to publisher status. Many of these cases involve offenses other than copyright infringement. In the U.S. such offenses would fall under the CDA, not the DMCA, and it is clearer that an interactive service provider must be responsible for creating or developing the content before it loses immunity. This result is consistent with the better-reasoned line of French cases, such as the appellate court decision in *Dailymotion,* holding that mere organization of a hosting website and an advertising-based business model is insufficient to make an ISP a publisher.

When such a case involves copyright infringement, as in the French MySpace case, it exposes an ISP to monetary liability for failing to prevent a copyright infringement, without specific notice and takedown protections. At least, however, monitoring and filtering to prevent copyright infringement is technically feasible and practicable using today's sophisticated screening technology. In fact, at least one ISP, Google's YouTube subsidiary, is beginning to offer voluntary screening on a test basis in cooperation with copyright owners.[56] But the ISP needs to know at least the universe of specific material subject to copyright protection to use these tools to detect infringement. The cases involving content found illicit for reasons other than copyright infringement, like the recent Italian case finding Google executives liable for violation of privacy rights, present a greater dilemma. While monitoring and filtering content posted by users for a known set of copyrighted works is feasible and arguably practicable, the prospect of monitoring and filtering content for violations of privacy, anti-Fascism or other anti-hate laws, defamatory content, or content that may be found "illicit" under a plethora of other European national laws is indeed a harrowing pros-

pect. ISP interests need to have this issue addressed in international treaty negotiations, but they are likely to confront vigorous opposition from some national interests.

Liability for Repeat Infringements

In cases involving the prevention of repeat infringement, such as the French *Google Video* case, the result does not seem out-of-line with safe harbor provisions. Viacom, Inc. recently pursued a strategy using Internet sniffing technology to detect infringements of its works on an ISP network and then issued tens of thousands of "robotically generated" takedown notices to the ISP. The effect as a practical matter is to impose a form of technical screening on an ISP.[57] In other words, when a copyright owner has complied with notice and take down requirements as to specified infringing materials under the DMCA, an ISP may be required, as a practical matter, to implement targeted monitoring and filtering to detect and prevent repeat infringements with respect to those specifically identified works.

Contributory or Vicarious Liability

An injunction imposing a form of monitoring and filtering may be imposed in the U.S. in cases of contributory or vicarious liability at the preliminary injunction stage, or permanently, if it is found that the DMCA safe harbors do not apply. The Belgium *SABAM* case is, however, remarkable. Under the DMCA, a U.S. court could order an IAP qualifying for the "mere conduit" safe harbor to disable access "to a specific, identified online location outside the U.S.," similar to the relief granted in the *Pirate Bay* case in Denmark. But the DMCA would not permit the form of injunction granted in *SABAM*, which required general monitoring and filtering to prevent illegal peer-to-peer file sharing of copyrighted works on websites the IAP did not control or even host and where there is no indication of conduct by the IAPs giving rise to contributory or vicarious liability. Due to the limitations on injunctive relief in the DMCA, an ISP that qualifies for any one of the safe harbors and does not induce, otherwise materially and knowingly contribute, or control and profit from infringements should not be at risk of such injunctive relief in the U.S.

Modern filtering technology is increasingly being used to monitor and police the Internet. Its application to copyright infringement presents only one set of issues. Others arise in the context of the privacy of communications, state censorship, and network neutrality, to name only the most notable. The overarching challenge is to use the technology wisely to promote the welfare of society, while not undermining the Internet's role as a haven for innovation, free expression and association. ▯

The views expressed in this article are personal to the author and do not necessarily reflect the views of the author's firm, the State Bar of California, or any colleagues, organization, or client.

Bill Harrelson is associated with Tobin Law Group, PC, www.tobinlaw.us, practicing business, regulatory, and intellectual property law with emphasis in communications, the Internet, and ecommerce transactions, compliance, strategic planning, and litigation. Formerly Bill was senior counsel for MCI's Western Region. He will have received a master's degree in intellectual property law by the time this article goes to press. Mr. Harrelson can be contacted at bill@tobinlaw.us.

Endnotes

1. The French Official Journal of 22 June 2004 contained the "Loi N° 2004–575 du 21 Juin 2004 pour la confiance dans l'économie numérique."
2. *French ISPs angry over "Digital Economy" bill*, OUT-LAW News, 12/01/2004, quoting secretary-general of ISP rights group Reporters Sans Frontiers available at http://www.out-law.com/page-4191.
3. *See* 35 Cornell Int'l L.J. 189, 203–204, November, 2001–February, 2002, *Standards of Liability for Internet Service Providers: A Comparative Study of France And the United States with a Specific Focus on Copyright, Defamation, and Illicit Content*, Xavier Amadei ("Amadei Comparative Study"). The author cites to Articles 1382 and 1383 of the French Civil Code. For example, Article 1383 provides that "everyone is responsible for the damage caused not only by her own act but also by her negligence or carelessness."
4. Amadei Comparative Study, *supra* note 3 at 204–205, citing and discussing *Groupe Revue Fiduciaire v. EDV*, T. Com. Paris, Jan. 1, 1999 (defendant IAPs not liable for merely providing link to website containing unauthorized reproduction of copyrighted articles); and *Perathoner v. Pomier*, TGI Paris, May 23, 2001 (court found no ISP liability where it had no supervisory authority, direction, or control, merely provided a link to infringing website containing copyrighted musical work, and had no actual notice of the infringement).
5. *Id.* at 196–197 and 204–205, citing and discussing *Lefébure v. Lacambre*, TGI Paris, June 9, 1998 (ISP liable for failing to check content that violated privacy rights); *Halliday v. Lacambre*, CA Paris, 14e ch., Feb. 10, 1999, D. 1999 (privacy violation for posted nude pictures of model); and *Lacoste v. Société Multimania*, TGI Nanterre, Dec. 8, 1999 (holding that "the ISP has a general obligation of cautiousness and diligence. It has the responsibility to take the necessary precautions to prevent the infringement of third parties' rights and it has to take reasonable measures of information, vigilance, and action.").
6. Amadei Comparative Study, *supra* note 3 at 204, citing and discussing *Société Multimania v. Lacoste*, CA Versailles, 12e ch., June 8, 2000, D. 2000, IR 270.
7. *See Yahoo! Inc. v. La Ligue Contre le Racisme et l'Antisemitisme*, 433 F.3d 1199, 1202–1204, 1219 (9th Cir. 2006)("*Yahoo!*") for a description of the French court's decision in *Union des Etudiants Juifs de France & Ligue Contre le Racisme et L'Antisémitisme v. Yahoo!*

Inc. & Yahoo France, Tribunal de grande instance [T.G.I.] [ordinary court of original jurisdiction] Paris, May 22, 2000 (Fr.) [hereinafter LICRA-May], available in English at http://www.lapres.net/yahen.html).

8. Article 6 applies to providers of "communication to the public by electronic means" to include "'online communication to the public' covering any transmission of digital data that does not have the characteristic features of private correspondence in response to an individual request, by means of a process of electronic communication allowing the mutual exchange of information between the sender and the receiver." *France Act on Confidence in the Digital Economy Adopted*, Amélie Blocman, Légipresse available at http://merlin.obs.coe.int/iris/2004/6/article23.en.html.
9. *Alert-Law on Confidence in the Digital Economy: first legal action on the responsibility of ISPs International, Freedom of Expression eXchange (IFEX)*, 18 November 2004 available at http://www.ifex.org/france/2004/11/18/law_on_confidence_in_the_digital/.
10. The Court found them immune from liability because with respect to the stored information they lacked "knowledge of their illicit nature or facts and circumstances revealing this character…." 84 NTDLR 331, 337, Opting Out of the Internet in the United States and the European Union: Copyright, Safe Harbors, and International Law, Hannibal Travis (November, 2008), citing at n. 238 Tribunal de grande instance [T.G.I.] [ordinary court of original jurisdiction] Paris, Oct. 29, 2007, http://www.juriscom.net/documents/tgiparis20071029.pdf. The author notes that some *dicta* in the Court's opinion "could be construed as suggesting that liability might exist if the illegality was clearly apparent."
11. *Id.* at 378, citing at n. 240, Cour d'appel [CA] [regional court of appeal] Versailles, Dec. 12, 2007, http://www.juriscom.net/documents/caversailles20071212.pdf.
12. Law of July 29 1982 on audiovisual communication.
13. Article 6(V) of the Law on Confidence in the Digital Economy.
14. 47 U.S.C. § 230(c)(1).
15. Compare *Chicago Lawyers' Comm. for Civ. Rights Under Law, Inc. v. Craigslist, Inc.*, 519 F.3d 666 (7th Cir. 2008) with *Fair Hous. Council v. Roommates.com, LLC*, 521 F.3d 1157 (9th Cir. 2008)(*en banc*).
16. 47 U.S.C. § 230(c)(2).
17. *See* Web 2.0: Aggregator Website Held Liable as Publisher, Contributed by Franklin, International Law Office, June 26 2008, available at http://www.internationallawoffice.com/Newsletters/Detail.aspx?g=4b014ec1-b334-4204-9fbd-00e05bf6db95&redir=1.
18. *Marie B v Wikipedia Foundation*, Paris Tribunal of First Instance, October 29 2007.
19. *Les Arnaques.com v Editions Régionales de France* , Versailles Court of Appeal, December 12 2007.
20. *eBay Europe v SARL DWC*, Paris Court of Appeal, November 9, 2007.
21. *See* discussion of *Lafesse vs./ YouTube* in "LaFesse v.YouTube: Applying the status of Host to videosharing site," a` la une, Societe D'Avocats, January 1, 2009, available at http://www.pdgb.com/uploads/tx_pdgbbdd/PI_NTIC_Janvier_2009_GB.pdf. YouTube was nevertheless found liable for damages due to its failure to comply with a requirement of the DEL that hosting providers collect and maintain data (name, address and telephone number) allowing identification of any person responsible for the creation of the hosted content. The court further cautioned that once the host ISP is informed of the illicitness of the content, it must act promptly to remove the material or block access to it. To allow the host ISP to avoid repeated uploading of the content, the copyright owner must describe the disputed content, its precise location and the reason it must be withdrawn.
22. *See* Web 2.0: *Aggregator Website Held Liable as Publisher,* Contributed by Franklin, International Law Office, June 26 2008, available at http://www.internationallawoffice.com/Newsletters/Detail.aspx?g=4b014ec1-b334-4204-9fbd-00e05bf6db95&redir=1.
23. *See* discussion of the case *Jean Yves L. dit Lafesse v. MySpace,* Tribunal de Grande Instance de Paris, Ordannance de refere (June 22, 2007), "Internet Law—Developments in ISP Liability in Europe," Internet Business Law Services ("ISP Liability in Europe"), E-Commerce University- Diploma Programs- Student Contributions: Stephen W. Workman, Esq. (August 24, 2008) available at http://www.ibls.com/internet_law_news_portal_view.aspx?id=2126&s=latestnews.
24. irisplus, Legal observations of the European Audiovisual Observatory, Issue 2009-4, "Filtering the Internet for Copyrighted Content in Europe," Christina Angelopolous (March 2009) ("Filtering the Internet in Europe") at page 3; available at http://www.obs.coe.int/oea_publ/iris/iris_plus/iplus4_2009.pdf.en.
25. *Id*. at 5.
26. *See* Paris Court of Appeal holds that Dailymotion is a host and did not have knowledge of infringing material, Anne-Sophie Lampe, Bird and Bird (October 27, 2009) available at http://www.twobirds.com/English/News/Articles/Pages/Paris_CourtofAppeal_Dailymotion_host.Aspx.
27. *See* discussion of *Google Video* case, *SARL Zadig Productions, Jean-Robert Viallet et Mathieu Verboud v Sté Google Inc. et AFA*, Tribunal de Grande Instance de Paris (October 19, 2007) in "ISP Liability in Europe," *supra,* and "Filtering the Internet in Europe," *supra* at 4.
28. *Id.*
29. *See* discussion of *SABAM v SA Scarlet (anciennement Tiscali), Tribunal de Première Instance de Bruxelles*, (June 29, 2007) in "Filtering the Internet in Europe," *supra* note 24, at 5.
30. IFPI, IFPI hails court ruling that ISPs must stop copyright piracy, July 4, 2007. www.ifpi.org/content/section_news/20070704b.html.
31. *See* discussion of *FPI Danmark mod DMT2 A/S*, Frederiksberg Byrets kendelse (January29, 2008) in "Filtering the Internet in Europe," *supra* note 24, at 6.
32. *See* discussion of Court of Bergamo, *Sezione penale del dibattimento in funzione di giudice del riesame*, Ordinanza of 24 September 2008, in 'Filtering the Internet in Europe," *supra* note 24, at 6.
33. http://googleblog.blogspot.com/2010/02/serious-threat-to-web-in-italy.html.
34. http://www.businessworld.ie/livenews.htm?a=2560421.
35. http://www.nytimes.com/2010/02/25/technology/companies/25google.html.
36. http://online.wsj.com/article/SB10001424052748704240004575084851798366446.

html.

37. *See* France Approves Wide Crackdown on Net Piracy, New York Times, Eric Pfanner, October 22, 2009, available at http://www.nytimes.com/2009/10/23/technology/23net.html?_r=1.
38. *See* French Constitutional Council Validates Anti-Piracy Law, October 22, 2009, Global | Digital and Mobile, Aymeric Pichevin, available at https://blog.perfect-privacy.com/2009/10/25/french-constitutional-council-validates-anti-piracy-law/comment-page-1/.
39. *See* New York Times, *supra* n. 37.
40. *See* France: Antipiracy Law Is Passed, momento 24, September 16, 2009, available at http://momento24.com/en/2009/09/16/france-anti-piracy-law-is-passed/.
41. *See* Internet Law—Developments in ISP Liability in Europe, Internet Business Law Services, available at http://www.ibls.com/internet_law_news_portal_view.aspx?id=2126&s=latestnews
42. *See* France adopts three-strikes law for piracy, by Greg Sandoval, October 22, 2009, available at http://news.cnet.com/8301-31001_3-10381365-261.html.
43. *See* Britain Passes Strong Anti Piracy Law, Kris Erickson, November 23, 2009, available at http://www.pspworld.com/sony-psp/news/britain-passes-strong-anti-piracy-law-011991.php?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+pspworld+%28PSP+World+-+PSP+news+by+fans+for+fans%21%29.
44. 15 U.S.C. § 512(j)(1)(A) and (B). Even in granting these limited forms of relief a court must weigh specified considerations: 1) whether the injunction would "significantly burden" the ISP or its operations; 2) the magnitude of the harm to the copyright owner in the absence of an injunction; 3) whether implementation would be "technically feasible and effective" and "not interfere with access to noninfringing material at other online locations;" and 4) "whether other less burdensome and comparably effective means" are available. 15 U.S.C. § 512(j)(2).
45. 15 U.S.C. § 512(i)(1)(A).
46. "Filtering the Internet in Europe," *supra* note 24, at 3.
47. 15 U.S.C. § 512(i)(2).
48. *A&M Records, Inc. v. Napster, Inc.*, 114 F.Supp.2d 896, 919, n. 24 (N.D. Cal. 2000). While the applicable safe harbor in the case was in § 512(d) applying to providers of information location tools, the same requirements and reasoning apply to the hosting safe harbor in § 512(c).
49. *A&M Records, Inc. v. Napster, Inc.*, 239 F.3d 1004, 1025 and 1029 (9th Cir. 2001).
50. *Id.* at 1027.
51. *See A&M Records, Inc. v. Napster, Inc.,* 284 F.3d 1091 (9th Cir. 2002) and underlying injunction in *A&M Records, Inc. v. Napster, Inc.*, not reported in F. Supp.2 d, 2001 WL 227083 (N.D. Cal. 2001).
52. *See* 15 UCLA Ent. L. Rev. 139, 140-141(Summer 2008), "Protecting Copyrights at the 'Backbone' Level of the Internet" ("Protecting Copyrights at the Backbone,"), Schleimer, Joseph D; and Electronic Commerce, 3d Edition, at 227–228, 272–274 and 283, Ronald J. Mann, Aspen Publishers (2008).
53. "Protecting Copyrights at the Backbone," *supra* note 52, 15 UCLA Ent. L. Rev. 139 at 142 and 162–168.
54. *See* 18 FDMIPMELJ 633, at 667–674, "Internet Packet Sniffing and Its Impact on the Network Neutrality Debate and the Balance of Power between Intellectual Property Creators and Consumers," (Spring 2008). An ISP considering implementing voluntary filtering should carefully structure its offering, investigate and consider the impact on its exposure to liability. A treatment of the issues is not possible within the confines of this article. But the provisions of the DMCA allowing ISPs to implement a copyright owner's rights management tools and the "Good Samaritan" immunity granted by § 230(c)(2) of the CDA arguably allow most risk to be avoided. *See* "Protecting Copyrights at the Backbone," *supra* note 52, at 166–167.
55. *See Lenz v. Universal Music Corp.*, 572 F. Supp. 2d 1150 (N.D. Cal. 2008). This decision suggests a copyright owner must investigate whether a suspected infringement is a fair use before issuing a takedown notice or face potential liability for misrepresentation under DMCA § 512(f). It puts a kink in the copyright owner strategy of issuing numerous automatically generated takedown notices to an ISP. The decision is extremely controversial and the subject of numerous law review and journal articles. *See, for example,* 13 NO. 7 J. Internet L. 3, at 4, Preventing Illegal Sharing of Music Online: The DMCA, Litigation, And A New, Graduated Approach, William Sloan Coats, Julieta L. Lerner, and Eric Krause, Aspen Publishers, Inc (January, 2010); and 17 JIPL 147, Let's Not Go Crazy: Why Lenz V. Universal Music Corp. Undermines the Notice and Takedown, Mareasa M. Fortunato (Fall, 2009).
56. Miguel Helft, Google Tries System to Halt Video Pirating, Int'l Herald Tribune, Oct. 17, 2007.
57. "Protecting Copyrights at the Backbone," *supra* note 52, citing and discussing *Viacom Int'l, Inc., v. YouTube, Inc.*, No. 07CV2103, 2007 WL 775611 (S.D.N.Y. Mar. 13, 2007).