Richmond Journal of Global Law & Business

Volume 12 | Issue 2 Article 2

2013

International Covergence on the Need for Third Parties to Become Internet Copyright Police (But Why?)

Dennis S. Karjala
Arizona State University, Sandra Day O'Connor College of Law

INTERNATIONAL CONVERGENCE ON THE NEED FOR THIRD PARTIES TO BECOME INTERNET COPYRIGHT POLICE (BUT WHY?)

Dennis S. Karjala
Jack E. Brown Professor of Law
Sandra Day O'Connor College of Law
Arizona State University

TABLE OF CONTENTS

I. INTRODUCTION

The inexpensive, rapid, and massive copying possibilities that digital technologies and the Internet make available have brought issues of enforcement of copyright and related intellectual property rights into strong focus. Rightowners, of course, retain all of the rights they have always had against infringers whom they can identify and who are amenable to enforcement measures, such as litigation. The infringers are often not so easy to find, however, so rightowners would like to be able to engage the assistance of other participants in the processes in which infringements are taking place. Most of the initial focus was on Internet Service Providers (ISPs) and website operators, but recently banks, advertisers, and other participants in Internet commerce have been the object of judicial and legislative attention aimed at inducing greater responsibility on the part of these participants to uncover and prevent copyright infringement on the Internet.

Governments, too, have been active in both civil and criminal enforcement.

The fundamental question is the extent to which copyright owners should be able to enlist the assistance of third parties or government in the enforcement of their rights under copyright law.[1] In the United States, a major "hook" for inducing private enforcement activity by third parties is the notion of secondary liability: contributory infringement and vicarious liability. Applying law from the analog world, courts have developed a kind of "rule of reason" approach to secondary liability, which is now partially codified and supplemented in the case of ISPs by § 512 of the U.S. Copyright Act. Courts in other countries, however, have addressed many of the same issues as the U.S. courts and largely seem to be arriving at similar conclusions. Courts everywhere are trying to balance the interests of content owners in intellectual property rights enforcement against user interests in matters like privacy, free expression, transparency in regulatory processes, and third party interests in being free to adopt business models with minimal interference from government. In that sense, we are seeing something of an international "convergence" in the approach to third party liability. The question then arises, however, why we are involved in this kind of policy balancing at all: How did it become accepted that private third parties should be part of the copyright enforcement scheme?

II. BACKGROUND ON U.S. APPROACHES

United States law has long separated primary and secondary copyright infringement. Primary infringement occurs when the accused, without authorization, performs acts that lie within one of the copyright owner's exclusive rights.[2] Secondary infringement is further divided into contributory infringement and vicarious liability.[3] Both

---

[1] I refer herein often to copyright rights, but trademark rights too have been the focus of judicial activity in some important cases. Other intellectual property rights, such as those arising under trade secret or patent law, have yet to raise most of the questions that we are seeing with respect to drafting third parties into the intellectual property enforcement effort in the context of the internet.

[2] These are the exclusive rights to make "copies" of the work, to produce derivative works based upon the protected work, and to publicly distribute, perform, and display the work. 17 U.S.C. § 106(1)-(5). In addition, § 106(6) gives a limited public performance right for digital sound recordings.

[3] Recent Supreme Court jurisprudence has introduced a third category of secondary liability, generally known as "inducement." Metro-Goldwyn-Mayer Studios, Inc. v. Grokster, Ltd., 545 U.S. 913, 935-37 (2005). Few object to finding liability when the level of subjective encouragement of copyright infringement required for inducement liability is demonstrated. Unless otherwise noted, I assume herein that facts sufficient for an inducement liability holding are absent.

require that there be a primary infringement by someone other than the accused. A person is liable for contributory infringement if he has knowledge of the primary infringing activity and, in light of that knowledge, materially contributes to the primary infringement.[4] A person is vicariously liable if he has the right and ability to control the primary infringer's acts and receives a direct financial benefit from the infringement.[5] Courts attempting to apply these long-standing principles in the digital age have struggled both to distinguish between primary and secondary liability and to apply the various elements of contributory infringement and vicarious liability to the facts before them.

The seminal Internet case got no further than the District Court for the Northern District of California, but it has served as the model for most subsequent judicial interpretations and for the specific statutory amendment that now constitutes section 512 of the Copyright Act. *Religious Technology Center v. Netcom On-Line Communication Services, Inc.*[6] involved the unauthorized posting of copyright protected materials to a digital bulletin board that was accessible via the Internet. The primary infringer was one Erlich, whose Internet access provider Klemesrud operated the bulletin board in question. Klemesrud, in turn, connected to the Internet through Netcom, the ISP.

The court first held that storage by the primary infringer of uploaded copies on an ISP's computer system was not a direct infringement by the ISP of the copyright owner's exclusive right to make copies. Direct infringement of the reproduction right requires a volitional act that is lacking where a defendant's system is used by a third party to create a copy.[7] The court was worried that any other approach "would hold the entire Internet liable for activities that cannot reasonably be controlled."[8] The question of *who* makes the infringing copy when a customer uses the defendant's system has arisen with some frequency, and courts have uniformly followed *Netcom* in requiring a degree of volitional activity[9] for a finding of direct infringement.[10]

---

[4] *E.g.*, Gershwin Pub. Co. v. Columbia Artists Mgt., Inc., 443 F.2d 1159, 1162 (2d Cir. 1971).

[5] *E.g.*, Shapiro, Bernstein & Co. v. H.L. Green Co., 316 F.2d 304, 306 (2d Cir. 1963).

[6] Religious Tech. Ctr. v. Netcom On-Line Commc'n Servs., Inc., 907 F. Supp. 1361 (N.D. Cal. 1995).

[7] *Id*. at 1369-70.

[8] *Id*. at 1372.

[9] *E.g.*, Cartoon Network LP v. CSC Holdings, Inc., 536 F.3d 121, 131-32 (2d Cir. 2008); Costar Group, Inc. v. Loopnet, Inc., 373 F.3d 544, 548 (4th Cir. 2004).

[10] The *Netcom* court also held that Netcom did not directly infringe the exclusive rights of public distribution or display. Emphasizing that Netcom neither created

The primary focus now, however, is on secondary liability, and here again the *Netcom* case established the analytical framework. For vicarious liability, the court concluded that Netcom's right and ability to control its downstream users, like Erlich and Klemesrud, involved material issues of fact but that, in any event, Netcom's policy of charging a fixed fee regardless of whether the material was copyright infringing precluded a finding of direct financial benefit.[11] This is another point on which most, if not all, U.S. courts have concurred.

The trickiest issue in *Netcom* was that of contributory infringement. On the sub-issue of whether Netcom had knowledge of Erlich's infringement, the court concluded that notice from the copyright owner at least raised a fact question of whether Netcom learned about the infringing activities in time to do something about them. If that was the case, Netcom could be liable contributorily because Netcom always had control of its system. Moreover, Netcom's participation in the infringing activity would constitute a material contribution if the facts showed that Netcom was "able to take simple measures to prevent further damage to Plaintiffs' copyrighted works."[12] Thus, after *Netcom*, the contributory infringement question was whether the ISP had received actual notice of specific infringing activity and was in a position to take reasonable action to do something about it.

Logically, it is unclear how the simplicity or reasonableness of the defendant's actions to prevent infringement is related to the issue of materiality. The importance of the ISP's contribution to the infringing activity seems independent of how easy or difficult it is for the ISP to stop the infringement once it has knowledge. In such approaches we see the growth of the law. The court could have said that the ISP's contribution is simply not material, much as the Ninth Circuit did later with respect to the participation of credit card companies in payments schemes for copyright-infringing materials.[13] This would leave the ISP out of the copyright enforcement picture altogether. Or the court could have held that supplying the means to copy and widely

---

nor controlled the content of the posting but only provided access to the internet, the court concluded that it would not make sense to hold the ISP liable. Netcom did no more than what every other internet server does, and to hold Netcom liable would expand the net of copyright infringement much too broadly. As a matter of legal doctrine, the court held that where the system merely stores and passes the information on as a conduit, the system does not "cause" the information to be distributed or displayed. Rather, it is the infringing user of the system who causes these effects and is the one who should be directly liable for copyright infringement. Consequently, the ISP was not a direct infringer of copyright. *See* Netcom On-Line Commc'n Servs., Inc., 907 F. Supp. at 1371.

[11] *Id*. at 1376-77.

[12] *See generally id.*

[13] *See infra* notes 44-50 and accompanying text.

distribute materials, some of which are known to be infringing, was clearly material. This might make a good deal of sense in the abstract, but could easily end up "holding the entire Internet liable," throwing out the baby of millions of perfectly valid Internet transactions with the bath water of relatively few infringements. So, the court sought and found a middle ground, namely, a requirement that the ISP with knowledge take reasonable measures to stop the infringing activity. As shown through most of the rest of this article, the court seems to have struck a responsive chord, as both Congress and the courts have followed closely.

Congress relied on the *Netcom* case to draft a much more precise, and complex, amendment to the Copyright Act to cover ISP liability. Adopted in 1998 as part of the so-called "Digital Millennium Copyright Act," section 512 of the Copyright Act[14] protects any ISP that meets the conditions of one or more of the section's four "safe harbors" from liability for monetary damages for copyright infringements that take place using parts of the ISP's system. The statute also limits the availability of injunctive relief against ISPs who are immunized from monetary liability under one of the safe harbors.[15]

Section 512 is a complex statutory provision, but its basic operation can be understood by breaking it down into its constituent pieces.[16] It begins, in subsections 512(a), (b), (c), and (d), with the four safe harbors themselves, which apply, respectively, to (a) "conduit" ISPs who connect customers to the Internet and make no permanent copies or any selection of transmitted material or recipients, (b) ISPs who "cache" or temporarily store material at their sites for increased technological efficiency, (c) web hosts or bulletin board operators, such as Klemesrud in the *Netcom* case, and (d) ISPs involved in providing Internet links. Each subsection defines the types of activity that are immunized from damages claims and the specific conditions that must be met to qualify for each of those particular immunities. Several of these safe harbors require the ISP to take affirmative action to disable access to or remove infringing material of which it is given notice, and section 512(g) permits ISPs to replace the material or re-enable access to it upon receipt of an appropriate counter-notice affirming that the material was removed or disabled by mistake or misidentification. Section 512(i) then sets additional conditions for eligibility that are applicable to all four safe harbors, the most important of which requires

---

[14] 17 U.S.C. § 512.

[15] 17 U.S.C. § 512(j).

[16] Dennis S. Karjala, *Liability of Internet Service Providers under United States Law*, JURISPRUDENCIA, 2006, at 11.

that ISPs implement a policy of terminating clients who are repeat infringers.[17] Other provisions supplement this basic structure.

Many cases have litigated the detailed provisions of section 512. Of primary interest here is the requirement under subsections (b)-(d) that the ISP (A) not have actual knowledge of infringing material, be unaware of facts from which infringing activity is apparent ("red flag" knowledge), or, upon obtaining such knowledge, act expeditiously to remove or disable access to the infringing material; (B) not receive any financial benefit directly attributable to the infringing activity; and (C) upon receiving notice of infringement, respond expeditiously to remove or disable access to the infringing material. We can think of this provision as a codification of *Netcom*'s conclusion that an ISP would be contributorily liable if it had knowledge of infringing activity and failed to take simple or reasonable steps to stop it. This is important because the fundamental issue has appeared in trademark cases, and liability has been asserted against actors in the Internet commerce environment who are not ISPs. The issue has also arisen, of course, in countries outside the United States. Section 512 only applies to copyright claims against ISPs under U.S. law, whereas the general principles of *Netcom* can be, and have been, applied more generally. In all these instances, the fundamental issue is the degree to which we as a society do and should compel third parties to contribute time, effort, and money to the enforcement of intellectual property rights held by content owners.

A. U.S. Copyright Cases under Section 512[18]

The Second Circuit in *Viacom Int'l, Inc. v. YouTube,*

---

[17] 17 U.S.C. § 512.

[18] For convenience, Section 512(c)(1) is set out here in its entirety:

> (c) Information Residing on Systems or Networks At Direction of Users.—
>
> (1) In general.— A service provider shall not be liable for monetary relief, or, except as provided in subsection (j), for injunctive or other equitable relief, for infringement of copyright by reason of the storage at the direction of a user of material that resides on a system or network controlled or operated by or for the service provider, if the service provider—
>
> (A) (i) does not have actual knowledge that the material or an activity using the material on the system or network is infringing;
>
> (ii) in the absence of such actual knowledge, is not aware of facts or circumstances from which infringing activity is apparent; or
>
> (iii) upon obtaining such knowledge or awareness, acts expeditiously to remove, or disable access to, the material;

Inc.[19] held that the statutory requirement to remove infringing materials upon learning of their existence at the site contemplated knowledge of specific infringing material, because otherwise the ISP would not know how to remove it.[20] The *Viacom* court, indeed, found *two* instances under section 512 in which the degree of specificity of the ISP's knowledge was at issue. The first was in section 512(c)(1)(A), which provides a safe harbor if the ISP (i) lacks actual knowledge of the infringing activity, (ii) lacks "red flag" knowledge of the infringing activity (that is, is unaware of facts or circumstances from which infringing activity is apparent), or (iii) upon obtaining actual or "red flag" knowledge, acts expeditiously to remove or disable access to the infringing material.[21] The court concluded that (A)(i)'s "actual knowledge" element contemplated knowledge of specific infringing material.[22] Viacom then argued that "red flag" knowledge under (A)(ii) did not require awareness of specific infringing activity, because if it did the provision would be superfluous. Under this reasoning, knowledge of generalized infringing activity would disqualify the ISP from the protection of the safe harbor. The Second Circuit, however, thought that losing the safe harbor upon the acquisition of only generalized knowledge of infringing activity would contradict the plain meaning of the statute, especially the removal requirement that kicks in once the ISP has the requisite degree of knowledge.[23] The difference between (A)(i) and (A)(ii), according to the Second Circuit, was not in the specificity of the knowledge but between an objective and subjective standard: If the ISP is subjectively aware of the infringing activity under (A)(i), a removal obligation is triggered under (A)(iii) regardless of whether the content owner has sent a notice.[24] On the other hand, (A)(ii) is an objective provision that looks to whether subjective awareness of the specific facts would have made the infringing activity "apparent" to a reasonable person.[25]

> (B) does not receive a financial benefit directly attributable to the infringing activity, in a case in which the service provider has the right and ability to control such activity; and
>
> (C) upon notification of claimed infringement as described in paragraph (3), responds expeditiously to remove, or disable access to, the material that is claimed to be infringing or to be the subject of infringing activity.,17 U.S.C.A § 512(c)(1)(West 2010)

[19] Viacom Int'l, Inc. v. YouTube, Inc., 676 F.3d 19 (2d Cir. 2012).

[20] *Id.* at 30-31.

[21] *Id.* at 30.

[22] *Id.* at 32.

[23] *See generally id*.

[24] *Id*. at 41.

[25] Viacom Int'l, Inc., 676 F.3d at 30-31.

The second instance in which the degree of specificity of the ISP's knowledge is at issue under section 512 arises from section 512(c)(1)(B), which denies the safe harbor to an ISP that receives a direct financial benefit from the infringing activity and that has the "right and ability to control" such activity. This portion of the statutory safe harbors verbally mimics the traditional common law standards for vicarious liability, which include no knowledge requirement. The *Viacom* court noted the theoretical difficulty posed by importing a specific knowledge requirement into the "right and ability to control" provision of section 512(c)(1)(B), in that such an approach would arguably make that provision duplicative of the actual knowledge provision of section 512(c)(1)(A).[26] On the other hand, to treat "right and ability to control" under the statute as a codification of the common law vicarious liability rule (which does not require knowledge of specific infringing activity, or even general knowledge that infringing activity is taking place) results in an even greater problem, because the very ability to do what the statute requires once the ISP has actual knowledge – that is, remove or disable access to the infringing material – is sufficient to show liability under traditional vicarious liability law by showing right and ability to control the activity. Thus, compliance with the *requirements* for the safe harbor under section 512(c)(1)(A) and (C) would *deny* the availability of the safe harbor under 512(c)(1)(B).

Because the safe harbor is available only when the requirements of each of its pieces, namely, 512(c)(1)(A), (B), *and* (C) are satisfied, the safe harbor would never be available where the elements of traditional vicarious liability are shown. The Second Circuit did not believe that this was the congressional intent and concluded that "right and ability to control" under 512(c)(1)(B) "requires something more than the ability to remove or block access to materials posted on a service provider's website."[27] The Second Circuit in *Viacom* declined to set a specific knowledge standard, however; it remanded the case for further consideration by the trial court of both the "right and ability to control" prong and the "direct financial benefit" prong of section 512(c)(1)(B).[28]

---

[26] *Id*. at 36.

[27] *Id*. at 38 (quoting Capitol Records, Inc. v. MP3Tunes, LLC, 821 F. Supp. 2d 627, 645 (S.D.N.Y. 2011)). Actually, the *Viacom* court's reasoning on this point ignores the second prong of vicarious liability, namely, direct financial benefit. Even if "right and ability to control" does not contain a knowledge element, many ISPs would fall outside the reach of § 512(c)(1)(B), namely, those who charge customers on a flat-rate basis regardless of the amount of use. It might arguably even exclude those who charge on a per/bit basis, provided the charges are the same for all materials sent, whether infringing or non-infringing.

[28] The court suggested that monitoring for the purpose of giving instructions on appearance and content as well as inducement of infringement might be the kind

UMG Recordings, Inc. v. Shelter Capital Partners LLC[29] involved the use by consumers of the system of the defendant, Veoh Networks, to upload and share video files. Some of these user-uploaded videos allegedly infringed UMG copyrights, and UMG asserted both direct and contributory infringement against Veoh. Veoh claimed a defense under section 512(c), the web host safe harbor, and the court first held that the eligibility language "by reason of the storage [on the defendant's system] at the direction of a user" applied even where, as in this case, the system not only stored exactly what was uploaded but also automatically reformatted the submissions to make them more accessible to others.[30]

UMG did not send any DMCA-compliant notices to Veoh, which would have given Veoh the URL information about infringing videos that would have made it easy for Veoh to take them down.[31] Rather, UMG argued that Veoh had general knowledge that many of the millions of videos available on its system contained copyright-protected material and were uploaded without authorization to the Veoh system.[32] This, UMG asserted, was "actual knowledge" of infringement under section 512(c)(1)(A)(i) and was also sufficient to raise a "red flag" under section 512(c)(1)(A)(ii) that infringing activity was "apparent." Because Veoh had not acted to remove such infringing materials in the face of such purported actual or "red flag" knowledge, as required by 512(c)(1)(A)(iii), it was not entitled to the benefit of the safe harbor. In other words, UMG's position was that general knowledge of *some* level of infringement was sufficient to trigger an obligation on the part of the ISP to find the offending material and disable access to it. The Ninth Circuit concluded that copyright owners were in

---

of "substantial influence" that could show a "right and ability to control." Viacom Int'l, Inc., *supra* note 19, at 38. A district court has interpreted "right and ability to control" in section 512 as going beyond the mere technological ability to remove or block access and requiring some participation like prescreening content, rendering "extensive" content advice to users, or editing content. Wolk v. Kodak Imaging Network, Inc., 840 F. Supp. 2d 724, 748 (S.D.N.Y. 2012) (involving a photo-sharing service allowing users to upload and share photographs and videos).

[29] UMG Recordings, Inc. v. Shelter Capital Partners, 667 F.3d 1022 (9th Cir. 2011), *superseded* UMG Recordings, Inc. v. Shelter Capital Partners, No. 09-55902, *slip opinion* (9th Cir. March 14, 2013). The superseding opinion was issued after rehearing by the panel but does not change the analytical approaches adopted by the court in its earlier opinion. For purposes of this article, the primary change is to follow closely the Second Circuit's decision in *Viacom*, if anything heightening the case for convergence.

[30] UMG Recordings, Inc., No. 09-55902 at 28.

[31] Indeed, it seems that whenever Veoh did get a DMCA-compliant notice, it removed the offending files. *Id*. at 28-29.

[32] *See id*. at 29-30.

a better position to identify infringing copies than ISPs, as evidenced by the notice provisions of section 512, and therefore that general knowledge that one's system was being used to share infringing materials was insufficient to deny the benefit of the statutory safe harbor to ISPs.[33] The court placed emphasis on section 512(m), which forbids statutory construction of the safe harbors as requiring ISP monitoring of its system for infringing activity.[34] The court also explicitly adopted the Second Circuit's distinction in *Viacom* between actual knowledge in 512(c)(1)(A)(i) and "red flag" knowledge in (A)(ii): (A)(i)'s actual knowledge standard is subjective and is met when the ISP is subjectively aware of specific infringing activity, while (A)(ii)'s "red flag" knowledge simply requires subjective awareness of facts that would make specific infringement apparent to a reasonable person.[35]

Veoh might still have been denied the safe harbor under section 512(c) had it received a direct financial benefit from the infringing activities (user uploads) and had the "right and ability to control" such activities.[36] As the Second Circuit concluded in *Viacom*,[37] if the statutory meaning is the same as the common law meaning, the safe harbor would never be available whenever the ISP would be vicariously liable under the common law test, because ISP agreements with users always give ISPs the legal right to police user activity.[38] Disabling access would in itself show the "ability to control," so the very requirement for protection of the safe harbor under (A)(iii) and (C) would *disqualify* from the safe harbor under (B).[39] The court believed Congress intended the safe harbor to apply even where the traditional elements of vicarious liability were present[40] and went on to conclude, following *Viacom*, that "right and ability to control" in the statute means "something more" than general ability to locate infringing material and terminate access.[41]

---

[33] *Id*. at 31.
[34] *Id*. at 32.
[35] *Id*. at 39.
[36] 17 U.S.C. § 512(c)(1)(B).
[37] Viacom Int'l, Inc. v. YouTube, Inc., 676 F.3d 19, 36-38 (2d Cir. 2012).
[38] *See* Mark A. Lemley, *Rationalizing Internet Safe Harbors*, 6 J. TELECOMM. & HIGH TECH. L. 101, 104 (2007).
[39] UMG Recordings, Inc., No. 09-55902 at 42-43.
[40] *Id*. at 45-47.
[41] *Id.* at 48. The court recognized that willful blindness – deliberate actions aimed at avoiding specific knowledge of infringing activity – would count as "knowledge" and deny the availability of the safe harbor. *Id*. at 34. Given the court's conclusion that the "right and ability to control" prong of vicarious liability was not satisfied, because of the absence of proof that Veoh had specific knowledge of infringing activity, the court did not address the other requirement of direct financial benefit. *Id*. at 40, n.16.

The important principle to be gleaned from the holdings of *Viacom* and *Shelter Capital* is that secondary liability on *both* traditional branches – contributory infringement and vicarious liability – requires knowledge of specific infringing activity and not merely generalized knowledge that some unidentified users have employed the system in an unidentified way to infringe copyrights.[42] The onus is on the copyright owner to inform the system operator not only of the general fact of infringement but also of specific information sufficient to permit the ISP to take action to stop the infringement by denying access to or disabling the infringing site. We might note that requiring action by the ISP after receiving notice does place a nontrivial burden on the ISP to participate in the enforcement of other people's copyright rights. It is, however, closely analogous to what we have long required under secondary liability principles in the analog world of people who are, in one way or another, connected to the activities of a copyright infringer.

A recent district court decision hints at the kind and level of surveillance courts may require of ISPs under section 512. In *Capitol Records, Inc. v. MP3Tunes, LLC*,[43] the defendant operated a system that allowed users to store music files in virtual lockers, from which the files could be played by the user with any Internet-connected device. Users could upload files stored on their personal hard drives and could transfer music files to their lockers from third party websites. A second website operated by the defendant allowed users to search for music files on the Internet and "sideload" such files into their individual lockers. Plaintiffs identified websites from which Defendant's users had sideloaded protected music files and gave section 512 compliant notices to Defendant demanding the removal from users' lockers of the songs that had been sideloaded from the identified websites. Because Defendant kept track of the source and web address for each sideloaded song, the court concluded the notice gave sufficient information to permit finding the infringing music in individual lockers and removing or disabling access to it. The court generalized by saying that where ISPs allow the searching and storing of protected works in private accounts, the ISPs must keep track of the source and web address of stored protected material, and they must take down such content upon receipt of a Section 512 compliant notice.[44]

---

[42] It is perhaps worth noting that if the traditional law of vicarious liability were to apply, not even the generalized knowledge of infringement on the defendant's system would be necessary to state a claim. Both Viacom and UMG vigorously asserted such knowledge, perhaps because they sensed that a court would not be sympathetic to what would otherwise amount to a strict liability claim.

[43] Capitol Records, Inc. v. MP3Tunes, LLC , 821 F. Supp. 2d 627 (S.D.N.Y. 2011).

[44] *See id*. at 642-43. The court went on to hold that the safe harbor was available to defendant for works stored on or linked to defendant's system, other than works

The U.S. cases under section 512 thus show continued viability of the general approach in *Netcom* that ISPs must take reasonable steps to avoid or reduce infringing activity using their facilities; however, there is no ongoing general obligation to patrol the system to discover and root out infringement of which the ISP is otherwise unaware.[45] Section 512 has added many technicalities to make the notion of "reasonable steps" more precise. In most ways the statute has been highly successful, but the basic, intuitive approach of the *Netcom* court remains largely undisturbed.

B. U.S. Cases Outside of Section 512

In *Perfect 10, Inc. v. Visa International Service Association*,[46] the plaintiff sued various credit card companies for contributory and vicarious copyright infringement based on the processing of credit card payments by customers of third party websites that offered infringing copies of the plaintiff's copyright-protected photographs. Because the credit card companies did not qualify as ISPs under section 512,[47] the court applied the common law of secondary liability. Over a vigorous dissent, the Ninth Circuit majority found no contributory infringement because processing a credit card payment was not a material contribution to the actual infringing acts of reproducing and distributing the protected photos.[48] Similarly, the court found no vicarious liability be-

---

sideloaded from links identified in the takedown notices. *Id*. at 646. Defendant was, however, held contributorily liable for failing to block user access to infringing material in individual user lockers that had been identified in the notices. Defendant's system made a substantial contribution to the infringement and the notices gave actual knowledge of the infringement. *Id*. at 648-49.

[45] *See also* Perfect 10, Inc. v. Amazon.com, Inc., 487 F.3d 701, 729 (9th Cir. 2007). The Ninth Circuit did not reach the Section 512 issue but held that Google could be held contributorily liable to Perfect 10 under general secondary liability law "if it had knowledge that infringing Perfect 10 images were available using its search engine, could take simple measures to prevent further damage to Perfect 10's copyrighted works, and failed to take such steps." *Id*.

[46] Perfect 10, Inc. v. Visa Int'l Serv. Ass'n, 494 F.3d 788 (9th Cir. 2007).

[47] An earlier case in the Ninth Circuit also raised the issue of liability of a credit-card processor CCBill for handling payments relating to infringing photographs. Perfect 10, Inc. v. CCBill, LLC, 488 F.3d 1102 (9th Cir. 2007). In this case, section 512 was raised as a shield, and the Ninth Circuit remanded for a determination of whether CCBill qualified as an ISP under section 512(a). The court concluded that CCBill did not qualify under Section 512(d), because its services went far beyond mere information location and linking, and the infringement claim was not for the linking but for the processing of monetary payments. *Id*. at 1116-17.

[48] Visa Int'l Serv. Ass'n, 494 F.3d at 796. Because it found that defendants did not make a material contribution to the infringement, the court did not reach the issue of whether they had the requisite knowledge for contributory infringement. *Id*. at 795.

cause while the credit card companies had the right and power to cut off payments to operators of websites identified as infringers, they had neither right nor power to control operation of the actual systems that were used to effect the infringements by reproducing and distributing the protected photos.[49] While the arguments were necessarily set forth in doctrinal terms, the court was clearly worried that a decision against the credit card companies might have a drastic and negative effect on Internet commerce: "We evaluate Perfect 10's claims with an awareness that credit cards serve as the primary engine of electronic commerce and that Congress has determined it to be the 'policy of the United States (1) to promote the continued development of the Internet and other interactive computer services and other interactive media [and] (2) to preserve the vibrant and competitive free market that presently exists for the Internet and other interactive computer services, unfettered by Federal or State regulation.'"[50]

It is clear, as Judge Kozinsky's dissent in *Visa* repeatedly emphasizes,[51] that cutting off payments to websites that are allegedly offering infringing materials would likely help reduce the level of infringing conduct on the Internet. It is also clear that processing credit card payments makes a material contribution to concluding the transaction (whether the deal is for infringing material or not), at least in the sense that, but for the credit card payment, the transaction likely would not occur at all. Further, the nature of Internet transactions concerning photographs almost invariably means that the transaction itself involves multiple infringements (if unauthorized), as the digital file moves from the server on which it is stored (probably illegally), through multiple digital devices before ending up on the purchaser's hard drive. Nevertheless, the credit card companies have no way of knowing whether any *particular* transaction involves infringing material or, if it is infringing, whether the current plaintiffs are the copyright owners. Their choice, therefore, is either to cut off a given site's transactions completely or to process all of them, despite knowing that some of the processed transactions allegedly involve infringing materials. Framed this way, the issue is whether a third party credit card company lacking knowledge that any specific transaction

---

[49] *Id.* at 805. Having found that defendants lacked the right and ability to control the infringing activities, the court did not reach the issue of whether the credit card companies derived a direct financial benefit from the transactions. *Id*. at 806. It would seem, however, that they did have such an interest, because they charge a percentage of every transaction, so the more infringing transactions there are, the more money they make. Indeed, the dissent pointed to allegations that the defendants gave special treatment to the infringing sites because of the "unusual and substantial profits" they earned from such transactions. *Id.* at 820.

[50] *Id.* at 794 (citing 47 U.S.C. §§ 230(b)(1), (2)).

[51] *Id.* at 810 (Kozinsky, J. dissenting).

involves infringing material must cut off *all* transactions with the allegedly infringing site, including those in which the complaining party has no interest and including many that at least potentially are perfectly legitimate.

It is not surprising that the *Visa* case resulted in a deep division on the three-judge panel that heard it. Suppose money-laundering transactions are known to be going through a specific bank but there is no way to identify which specific transactions are illegal and which ones (presumably the majority) are not. Should a court, without legislative authority, order another bank to stop all business with the first bank – the one known to be used for money laundering? If this is problematic, it is even more so where the court order to stop doing business with a particular website is aimed at protecting *private* commercial interests, as in the case of infringing content.[52] Selecting between (1) allowing the payment processing for at least some infringing transactions and (2) closing down a site completely and thereby eliminating *all* transactions at that site going through that payment processor, whether infringing or not, forced the *Visa* court to go a step beyond the approach of *Netcom*. In *Netcom*, the ISP would have been liable had there been sufficiently specific knowledge of infringing activity and reasonable steps, which were available to the ISP, were not taken to stop the infringing activity.[53] *Visa* essentially says that shutting down an entire site to protect copyright rights of a single copyright owner is not a "reasonable step."[54]

Tiffany (NJ) Inc. v. eBay, Inc.,[55] was a trademark case, outside of section 512, that raised the same issue as the copyright cases dis-

---

[52] The Ninth Circuit majority expressly worried about the slippery slope – other providers of goods and services to businesses alleged to be copyright infringers, such as electric power companies and software services. *Id*. at 800. Judge Kozinsky, in dissent, dismissed this fear saying that utilities have an obligation to deliver services independent of contract and that software services generally have no contract that permits them to stop providing services on account of illegality. *Id*. at 821-22. Judge Kozinsky's argument may be relevant to the "right and power to control" prong of vicarious liability, although it would hardly seem to be determinative. It is wholly unconvincing on the "material contribution" prong of contributory infringement, because once either the power company or the software servicer has notice of infringement, each makes a material contribution to that infringement by supplying indispensable elements to the system used to effect the infringement.

[53] Religious Tech. Ctr. v. Netcom On-Line Commc'n Servs., Inc., 907 F. Supp. 1361, 1373 (N.D. Cal. 1995).

[54] *See* Visa Int'l Serv. Ass'n, 494 F.3d 7886.

[55] Tiffany (NJ), Inc. v. eBay, Inc., 600 F.3d 93 (2d Cir. 2010).

cussed above.[56] Here, the well-known online auction site eBay was sued by the famous designer and seller of high-end jewelry and other items, Tiffany's, for contributory trademark infringement by failing to stop allegedly widespread sales on the eBay site of counterfeit Tiffany products.[57] Given the absence of any statutory provision for contributory trademark infringement, the Second Circuit followed the Supreme Court's test looking to whether the alleged infringer continued to supply a product to a person who he knew or should have known was engaging in trademark infringement.[58] The evidence in the case showed that eBay promptly removed challenged listings, but Tiffany argued that eBay had knowledge that many listings not directly challenged also involved counterfeit Tiffany goods. The Second Circuit agreed with the district court that something beyond general knowledge that the site was used to sell counterfeit goods was necessary for eBay to be held liable for contributory infringement.[59] The court noted, but did not base its decision on, the incentives eBay already had to make strong efforts to minimize counterfeit transactions on its auction site. Many customers who purchased counterfeit goods complained to eBay, so it was in eBay's general interest to try to stop such activities. Indeed, eBay spent millions of dollars in an effort to minimize counterfeit transactions.[60]

III. NON-U.S. CASES

Cases from outside the United States, primarily Japan and the European Union, provide a general idea of what appears to be a significant degree of convergence in judicial treatment of the basic problem. The discussion herein, outside of Japan, Australia, and the United Kingdom, is based on summaries of decisions that have appeared in the literature.

---

[56] For a detailed analysis of this decision, *see* Justin Nicholas Redman, *Post Tiffany (NJ), Inc. V. eBay, Inc.: Establishing a Clear, Legal Standard for Online Auctions,* 49 JURIMETRICS J. 467 (2009).

[57] Tiffany also alleged direct trademark infringement, but the sale of at least some legitimate Tiffany goods on eBay was a noninfringing use of the Tiffany mark to describe the goods accurately. Tiffany, *supra* note 55, at 101. eBay's generalized knowledge of *some* counterfeit sales was relevant only to the contributory infringement issue, because it was undisputed that eBay promptly removed all specific listings that Tiffany challenged as counterfeit. *Id*. at 103.

[58] Tiffany (NJ), *supra* note 55, at 103 (citing Inwood Labs., Inc. v. Ives Labs., Inc., 456 U.S. 844, 854 (1982)). The *Inwood* Court would also find contributory infringement against one who intentionally induces another to infringe a trademark. *Inwood Labs*., 456 U.S. at 854. That prong of *Inwood* was not at issue in *Tiffany*. *Id*. at 104.

[59] *Id.* at 107.

[60] *Id*. at 109.

A. Australia

The High Court of Australia in *Roadshow Films Pty Ltd v. iiNet Ltd.*[61] faced the question of whether an ISP "authorised" copyright infringement by providing Internet connection services to customers who used the BitTorrent P2P file sharing system to exchange copyright protected films. While Australia has a statutory safe harbor scheme similar to that of the United States,[62] the defendant iiNet was ineligible for its protection,[63] so the court addressed the problem by applying general copyright principles. Under the Australian statute, the issue was whether the defendant had "authorised" the infringing activity.[64]

Plaintiffs argued that iiNet's technical and contractual relationships with its customers gave it indirect power to control the use of its Internet connection services, that this power to control was equivalent to "authorisation," and that an injunction should issue restraining iiNet from continuing to provide Internet connection services to each of some eleven specified accounts. The court framed the authorization issue as involving subsidiary questions of whether iiNet had the power to prevent the primary infringements and whether iiNet took reasonable steps to prevent infringements after receiving notice.[65] At least on the surface, this analysis appears similar to that of the *Netcom* court in the United States.

In the actual case, the Australian High Court concluded that iiNet had limited power to prevent infringement, namely, indirectly by terminating its contracts with infringing customers. Like the *Visa* credit card case in the United States, the Australian court may have deemed it excessive to shut down an entire site – including transactions in which the current plaintiffs had no copyright interest and even legitimate transactions — in the service of stopping a relatively small number of specific infringements. On the "reasonable steps" prong of the analysis, the High Court noted that a terminated account could engage another ISP and continue with the infringing activity, and if iiNet gave warnings it would be obliged to try to monitor the warned customers, which itself would require a detailed technical involvement with the BitTorrent technology.[66] The court thus seemed to believe that whatever iiNet did, it was unlikely to be effective. Moreover, the

---

[61] Roadshow Films Pty Ltd v. iiNet Ltd ., [2012] HCA 16, ¶ 4.

[62] *See generally* Australian Copyright Act §§ 116AA - 116AJ; *see* Roadshow Films, *supra* note 61, ¶ 25. The safe harbor limits remedies against ISPs but allows courts to require the ISP to terminate a specified account. *Id*. ¶ 13.

[63] *Id*.

[64] *Id.* ¶ 5.

[65] *Id*. ¶ 63.

[66] *Id*. ¶ 73-74.

High Court found some deficiencies in the notices of infringement that iiNet had received.[67] Therefore, the High Court dismissed the plaintiffs' appeal.

B. Japan

In the *Internet Mall Case*,[68] the operator of an Internet shopping mall was sued for trademark infringement based on the unauthorized use of Plaintiff's registered mark on various goods offered by one of the virtual "stores" in Defendant's mall. The lower court held that the Internet mall operator was not a party (*shutai*) to the infringing transactions between the store operator and his purchasing customers. On that ground the lower court found no trademark infringement on the part of the mall operator. The High Court did not directly address the question of whether the mall operator was a party to the transactions but said that the mall operator could be liable if, after getting knowledge of specific infringing activity, he failed to act to shut down or disable the site within a reasonable time. On the actual facts, the mall operator was not liable because he did act within a reasonable time after receiving notice.[69]

The High Court first noted that Internet shopping is a social benefit and most transactions do not involve trademark infringement. Moreover, the High Court reasoned, even where trademark rights are involved, the store owner may be the rightowner, he may be authorized by the rightowner, or the item may be a parallel import, so the fact that the item is available does not itself lead to a high probability

---

[67] *Id.* ¶ 78.

[68] Perfetti Van Melle S.p.A. v. Rakyten Corp., Heisei 22 (ne) No. 10076 (Tokyo Intellectual Property High Court, Feb. 14, 2012). A brief summary of this case, in English, may be found at Toshio Aritake, *Japan IPR Court Holds Internet Shopping Mall Liable for Infringement*, 26 WIPR 23 (Feb. 2012). Unfortunately, this report is not entirely accurate, because it states that the IPR court held both the mall operator and the vendor (virtual "store") liable whereas the lower court held only the vendor liable. In fact, the vendor was not a party to the lawsuit and, therefore, the holding of neither court reached the vendor, although the IPR court did state in dictum that the vendor would be liable. Moreover, as discussed in the text below, the IPR court found *no* liability of the mall operator on the actual facts and overruled the lower court only to the extent of stating that the mall operator *could* be liable if he did not act within a reasonable time after receiving notice of the infringing activity.

[69] *Intellectual Property High Court Ruled That Internet Shopping Mall Operators Can Be Found Liable for Trademark Infringement*, ITOH INT'L PATENT OFFICE (Feb. 24, 2012), http://www.itohpat.co.jp/e/ipnews/index.html. In this case, the mall operator acted within 8 days or less after receiving notice, which the court concluded was a reasonable time (without giving any more specific reasons). *Id.*

that the store owner is infringing.[70] Nevertheless, trademark infringement is also a crime under commercial law and regulations, so where an ISP has concrete knowledge of trademark infringement by a store operator, there is a possibility of contributory infringement.[71] The Internet mall operator also makes money from the store owner's operations, and where the operator is aware of infringing activity at a particular store, he has power under the contract with the store owner to delete the content or block access to the page. Thus, when the mall operator receives notice of infringement from a trademark owner, he has an obligation to make an immediate investigation. To the extent he fulfills this obligation, he is not liable for trademark infringement, but if he neglects it he bears the same responsibility for infringement as the storeowner.[72] There seems to be no substantial difference between the approach of the Tokyo IP High Court here and that of the U.S. Second Circuit in the *eBay* case, notwithstanding different statutory language and jurisprudential history.

C. European Union

Section 4 of the E-Commerce Directive[73] seems to be quite similar to section 512 of the U.S. Copyright Act, discussed above. Articles 12-14 of Section 4 insulate service providers who act as "mere conduits," engage in "caching," or provide information storage services ("hosting"), if the service provider complies with various conditions.[74] The "hosting" safe harbor applies when the service provider lacks actual knowledge of infringing activity and is unaware of facts or circumstances from which infringing activity is apparent or, upon obtaining such knowledge, acts expeditiously to remove or to disable access to the information.[75] Article 15 prohibits the establishment of a general obligation on service providers to monitor information that they store or transmit or actively to seek facts or circumstances indicating illegal activity.[76] The Court of Justice of the European Union has interpreted Article 15 to deny the demand of the Belgian copyright management company SABAM that a social network install a filter system to monitor all users for infringements of music and audiovisual works.[77]

---

[70] *See id.*

[71] *See* 2012 (ne) no.10076, *supra* note 68.

[72] *Id.*

[73] Council Directive 2000/31, 2000 O.J. (L 178) 1 (EC).

[74] *Id.* art. 12-14.

[75] *Id.* art. 14.

[76] *Id.* art. 15.

[77] Case C-360/10, SABAM v. Netlog NV., 2012 EUR-Lex CELEX LEXIS (Feb. 16, 2012).

The Court of Justice of the European Union (CJEU) has also interpreted much of this Directive in the context of alleged trademark infringements on an online marketplace. *L'Oreal SA v. eBay International AG*[78] involved much the same issue as the *eBay* case in the United States and the *Internet Mall* case in Japan. L'Oreal contended that eBay's internal procedures for preventing trademark infringement by sellers at its auction site were insufficient and brought suit in the United Kingdom when eBay did not respond satisfactorily to L'Oreal's demand to take stronger steps to prevent infringing activity. The English High Court held against L'Oreal on the issue of joint trademark infringement but referred that and other issues to the CJEU.[79]

On eBay's liability for infringing use of trademarks by sellers on eBay's site, the CJEU looked to the Directive. The court held that it was the sellers and not eBay who made infringing use of the trademarks by displaying goods on the website, so the liability of eBay would depend on the conditions of intermediary liability under the Directive. This harkens back to the *Netcom* court's refusal to hold the ISP liable for primary copyright infringement based on the posting of material by a customer. The CJEU interpreted Article 14, the "hosting" safe harbor, to apply only where the intermediary's services were provided "neutrally," via technical and automatic processing. The intermediary would not fall within Article 14 if it had knowledge or control over the presentation or if it provided assistance to its sellers by, for example, promoting or optimizing the sellers' offers. Moreover, even where Article 14 applies, the exemption is available by its terms only where the intermediary lacks actual knowledge of the infringement or, having obtained such knowledge, acts expeditiously to remove or disable access to the infringing data. Notice from the trademark owner is not conclusive on the knowledge issue, but it is a factor, presumably an important factor, for courts to consider in determining whether the intermediary should have known of the infringing activity.[80]

The *L'Oreal* case also addressed injunctions against ISPs under the Enforcement Directive, Article 11, which states in part, "Member states shall also ensure that rightholders are in a position to apply for an injunction against intermediaries whose services are used by a third party to infringe an intellectual property right."[81] The court

---

[78] Case C-324/09, L'Oreal SA v. eBay International AG, 2011 EUR-Lex CELEX LEXIS (July 12, 2011).

[79] Among the issues were trademark exhaustion, liability for removal of packaging materials, and the use of keyword advertising. *Id.*

[80] *Id.*

[81] Council Directive 2004/48, art. 11, 2004 O.J. (L 157) 45 (EC).

recognized that this provision was available against intermediaries not only to correct past infringements but also to prevent future infringements, but any such injunction must comport with Article 15 of the E-Commerce Directive, which expressly prohibits establishing a general obligation to monitor or to seek out facts indicating infringing activity. The court suggested suspension of the accounts of known infringers and orders making it easier to identify potentially infringing sellers as examples that might strike a fair balance between various rights and interests.

1. France

The French courts have already interpreted the *L'Oreal* standards and have come to apparently conflicting results for U.S. companies eBay and YouTube. In *eBay Inc. v. LVMH,*[82] the highest French court found that eBay played an active role in promoting various counterfeit goods and therefore did not qualify for the safe harbor under the E-Commerce Directive. While noting that eBay had knowledge and control over the data stored at the auction site, it is not clear that eBay actually knew that the data in question referred to infringing goods. If such knowledge is not required in France, the French rule for ISPs would be similar to the traditional U.S. rule for vicarious liability, meaning that the safe harbors of the E-Commerce Directive are not available against such claims. As noted above, the Second and Ninth Circuits in the United States have expressly held that the section 512 safe harbors do apply, at least to some extent, even in the context of traditional vicarious liability.[83]

On the other hand, in *YouTube LLC v. TF1*,[84] a French television broadcaster unsuccessfully sought liability from YouTube for the posting by YouTube members of infringing content on the YouTube site. Applying the *L'Oreal* standard of active participation, the court concluded that YouTube simply employed a statistical algorithm to rank videos in various categories, which is different from making a conscious choice or playing an active role in determining the content of the postings.[85]

It is not entirely clear how the *YouTube* and *eBay* cases in France are to be distinguished. It is probably true that YouTube is more automated because its primary purpose is to make videos availa-

---

[82] *Court of Cassation, May 3, 2012, c eBay. Louis Vuitton Malletier*, JURISCOM.NET (May 3, 2012), http://juriscom.net/2012/05/cour-de-cassation-3-mai-2012-ebay-c-louis-vuitton-malletier/.

[83] See *supra* text accompanying notes 34-57.

[84] Tribunal de grand instance de Paris [TGI] [ordinary court of original jurisdiction] Paris, 3e ch., May 29, 2012, No. 10/11205 (Fr.).

[85] *Id*. at 24-25.

ble, usually on a noncommercial basis. The commercial nature of eBay necessarily pushes it more deeply into the sales transactions that take place there. Still, it is not clear how eBay could determine which of the millions of items that change hands on its site daily are in fact counterfeit, at least without expenditure of a great deal of time and money on monitoring. Article 15 of the E-Commerce Directive says that such monitoring cannot be demanded of ISPs, so the question is whether eBay is different in any relevant respect from an ISP when it comes to the monitoring issue.[86]

2. Germany

The German courts seem to be taking a position that requires more of ISPs once they have notice of specific infringement. In *GEMA v. YouTube*,[87] the Hamburg Regional Court held that YouTube would not be liable for copyright-infringing content at its website unless, after receiving notice, it did not take immediate action to block the infringing videos. Had the court stopped there, its holding would be in line with the cases we have discussed thus far. However, the court went on to state that, once notice was received, YouTube was obligated to take measures to prevent additional violations, while clarifying that YouTube did not have an obligation to check all content on its site. Similarly, the German Federal Court in Karlsruhe held that a website operator does not have an obligation to check the content of an RSS feed hosted on its site, where the content of the feed is automatically published and its source identified.[88] In this case, the court said that the decisive factor was whether the website owner "adopted" the content, which could occur via editing the text or failing to clarify that the content came from a third party.

In *Atari v. RapidShare*, the highest court in Germany, the Bundesgerichtshof, affirmed the approach taken by the Hamburg Regional Court.[89] Atari sued RapidShare, a file hosting website, for copyright infringement based on the availability of infringing copies of some Atari video games on the site. The BGH denied direct infringement by RapidShare, but concluded that RapidShare could be liable if, once notified of the infringement, it failed to take sufficient measures to prevent access to the infringing material and also to prevent its be-

---

[86] 85B. Directive 2000/31/EC of the European Parliament and of the Council, *supra* note 73, art. 15.

[87] Jabeen Bhatti, *German Court Finds YouTube Responsible for Copyrighted Content When Given Notice*, 17 ELEC. COM. & LAW REP. 755 (Apr. 25, 2012).

[88] Jabeen Bhatti, *Court Rules Operator Not Liable Third Party Content Hosted via RSS Feed*, 26 WORLD INTELL. PROP. REP. 17 (July 1, 2012).

[89] Jabeen Bhatti, *Supreme Court Rules File Hosting Sites Must Do More to Prevent Infringement*, 26 WORLD INTELL. PROP. REP. 14 (Sept. 1, 2012).

ing uploaded again. The court suggested that RapidShare should have used filters to prevent a repeat infringement of the particular works in question and had a responsibility to search link collections on third party sites for links to the illegal file. Because in both of these German cases the requirement to take preventive measures seems to apply to specific works, this obligation does not directly conflict with Article 15 of the E-Commerce Directive's prohibition on general monitoring requirements, but the obligation is more than has been required of ISPs under section 512 by the U.S. courts.

3. United Kingdom

Twentieth Century Fox Film Corp. v. British Telecommunications PLC[90] involved a suit by film studios against the United Kingdom's largest ISP, British Telecommunications (BT), for copyright infringement based on the unauthorized availability for download by others of protected films at the site of one of BT's customers, Newzbin2. BT claimed protection as a "mere conduit" service provider under Article 12 of the E-Commerce Directive, as implemented in the United Kingdom. The main issue in the case was the meaning of "actual knowledge" in the Directive and in the U.K. implementing regulations. BT contended that liability required actual knowledge of a specific infringement of a specific work by an identified individual.[91] The court placed heavy reliance on the language of Article 8(3) of the Information Society Directive,[92] which is virtually identical to Article 11 of the E-Commerce Directive quoted above,[93] as implemented in section 97A of the U.K. statute.[94] That provision allows injunctions to issue against an ISP where the ISP has "actual knowledge of another person using their service to infringe copyright." It goes on to say that the court determines actual knowledge on the basis of the particular circumstances, including whether the ISP has received a notice of infringement and the extent to which the notice provides "details of the infringement in question."[95]

The court noted that under the E-Commerce Directive, an ISP with actual knowledge loses the benefit of the safe harbors of Articles 13 and 14, but this is not the case for "mere conduit" ISPs under Article 12, which suggested that "actual knowledge" should not be inter-

---

[90] Twentieth Century Fox Film Corp. v. British Telecommunications PLC, [2011] EWHC 1981 (Eng.).

[91] *Id*. ¶ 116.

[92] Directive 2001/29/EC of the European Parliament and of the Council 2001 O.J. (L167).

[93] *See supra* text accompanying note 81.

[94] Copyright, Designs and Patents Act, 1988 (Eng.).

[95] *Id.* c. 6, § 97A.

preted too restrictively.[96] Moreover, recital 59 of the Information Society Directive states "[R]ightholders should have the possibility of applying for an injunction against an intermediary who carries a third party's infringement. . .." Inferring a similar purpose to section 97A of the British statute implementing that part of the Directive, the court found a legislative intent to allow injunctions against an ISP who "carries" infringing material, because the ISP is best positioned to bring the infringing activities to an end.[97]

Perhaps most importantly for the court was the language of the statute in section 97A referring to "actual knowledge of another person using their service to infringe copyright." On the basis of this language, the court distinguished between *use of the service to infringe* from the infringements actually committed by such use.[98] The court concluded that, while "actual knowledge" can only be determined based on all the facts and circumstances, it is "not essential to prove actual knowledge of a specific infringement of a specific copyright work by a specific individual."[99] Thus, BT had actual knowledge that third parties were using its service to infringe.[100] The court also determined that it had the authority to grant the broad order sought by the film studios, which required the blockage of the entire Newzbin2 site to BT's subscribers rather than simply ordering BT to ensure that the specific content owned by the litigating studios was blocked.[101]

While the *Twentieth Century Fox* case in the United Kingdom appears on the surface to accept a lower threshold for "actual knowledge" than we have seen in the cases from the United States and other countries, it is perhaps important to point out that the remedy sought from BT was an injunction, not damages.[102] Even under section 512 in the United States, the DMCA safe harbor provisions apply largely to damages remedies sought against the ISP. Section 512(j)(1)(B) applies to the equivalent of "mere conduit" ISPs like BT, and limits injunctions to orders restraining the ISP from providing access to a subscriber or account holder who is using the service to infringe.[103] Consequently, the same broad order that was so fiercely contested in *Twentieth Century Fox* would likely be available in the United States without much discussion, assuming proof of similar facts.

---

[96] Twentieth Century Fox Film Corp., [2011] EWHC 1981 at ¶ 145.

[97] *Id*. ¶ 146.

[98] *Id*. ¶ 147.

[99] *Id*. ¶ 148.

[100] *Id*. ¶ 157.

[101] *Id*. ¶ 204.

[102] *Id.* ¶ 1.

[103] Digital Millennium Copyright Act (D.M.C.A.), § 512(b)(2)(E) (2012).

IV. NEW STATUTORY SCHEMES

In May 2011, after several years of controversial and somewhat opaque negotiations,[104] the proposed Anti-Counterfeiting Trade Agreement (ACTA)[105] was published. One of the ACTA drafters' major goals was to strengthen the weak enforcement requirements of TRIPS.[106] While it appears that ACTA will not be ratified, two of its provisions seem relevant to the current discussion on the liability of ISPs and other third parties for copyright infringement on the Internet. Article 8(1) would have required each treaty party to insure that "its judicial authorities have the authority to issue an order against. . ., where appropriate, a third party. . . to prevent goods that involve the infringement of an intellectual property right from entering into the channels of commerce."

Article 12 requires similar judicial authority to order "prompt and effective provisional measures" against a third party to prevent infringement. The Electronic Frontier Foundation has criticized ACTA on numerous grounds, one of which is that its language could be interpreted "to legitimize website filtering and blocking and Internet disconnection."[107] Article 12 of ACTA is surely susceptible to such an interpretation, but as the treaty left much to the discretion of the individual treaty parties, we cannot say with certainty that all or even many would have gone as far as feared by the Electronic Frontier Foundation.

The United States had its own legislative battle on many of the issues addressed by ACTA, the most widely discussed of which was Stop Online Piracy Act (SOPA).[108] SOPA first would have given criminal enforcement authority to the Attorney General to go after foreign sites that were directed at U.S. recipients, were violating the U.S. criminal copyright or federal trade secret provisions, and would have been subject to seizure were they U.S. sites.[109] Section 103 of SOPA focused on sites "dedicated to theft of U.S. property," that is, sites directed to users in the United States and designed primarily to infringe

---

[104] *See generally* Hilary H. Lane, *The Realities of the Anti-Counterfeiting Trade Agreement*, 21 TUL. J. INT'L & COMP. L. 183, 191-97 (2012) (describing international protests and several controversial effects of the act).

[105] Anti-Counterfeiting Trade Act (ACTA), Oct. 1, 2011, *available at* http://www.ustr.gov/acta (containing the text of the act).

[106] Peter K. Yu, *Enforcement, Enforcement, What Enforcement?*, 52 IDEA 239, 255 (2012). Professor Yu goes on to point out, however, that the ACTA obligations would themselves have been difficult to enforce. *Id.* at 264-65.

[107] *Anti-Counterfeiting Trade Agreement*, ELEC. FRONTIER FOUND., *available at* https://www.eff.org/issues/acta (last visited Feb. 18, 2013).

[108] Stop Online Piracy Act (S.O.P.A.), H.R. 3261, 112th Cong. (2011).

[109] *Id*. § 102(a).

U.S. copyright or trademark law.[110] The interesting thing about the civil provisions of SOPA in section 103 is that they were aimed at Internet payment providers and advertisers.[111] The evident goal of the statute was to enlist the assistance of these third parties in the enforcement of private intellectual property rights. After receipt of a statutory notice, payment providers would have had 5 days to suspend payment services involving U.S. customers and the offending foreign site, while advertisers would have had 5 days to stop advertising on the site, to stop making ads on behalf of the site, and to cease payments in either direction.[112]

The notice required by SOPA, among other details, had to identify the offending site either by domain name or Internet Protocol address.[113] The rightholder also had to include in the notice "specific facts" to support its claim that the site was dedicated to the theft of U.S. property and to "clearly show" that failure to take timely action would result in immediate and irreparable injury.[114] These requirements, had they been enacted into law and rigorously enforced by the courts, might have been difficult for rightholders to meet outside of the most blatant of infringers. For example, they are more demanding than the notice requirements under section 512 of the DMCA. On the other hand, especially in the case of payment sites, responding to a valid notice would likely require severing *all* transactional relations with the site, even those transactions that are not directed at U.S. users or that are perhaps not infringing at all. This could have resulted in correction measures highly disproportional to the wrong – for example, where an entire site is shut down but only a single page contains infringing materials.[115]

Lital Helman and Gideon Parchomovsky have recently proposed a new approach to liability for web hosts.[116] Under their proposal, hosts would be immune from liability provided they make use of the best filtering technology available on the market. They make a strong case that this approach would reduce costs and result in more rapid improvements in filtering technologies. The argument applies

---

[110] *Id.* § 103(a)(1).

[111] *Id*. § 103(b).

[112] *Id.* § 103(b)(1)-(2).

[113] *Id*. § 103(b)(4)(A)(ii).

[114] *Id*. § 103(b)(4)(A)(iii).

[115] Jeffrey A. Lindenbaum & David Ewen, *Catch Me if You Can: An Analysis of New Enforcement Measures and Proposed Legislation To Combat the Sale of Counterfeit Products on the Internet*, 32 PACE L. REV. 567, 638 (2012).

[116] Lital Helman & Gideon Parchomovsky, *The Best Available Technology Standard*, 111 COLUM. L. REV. 1194, 1194 (2011).

primarily only to web hosts, however, which leaves the problem open for a number of other players.[117]

V. WHY ARE WE DRAFTING PRIVATE PARTIES INTO THE COPYRIGHT POLICE FORCE?

At a basic level, these judicial and legislative efforts to enlist the assistance of third parties to enforce the copyright and other intellectual property rights held by others seems a bit strange. We do not demand that neighboring landowners assist one another in preventing trespass, and even patent law enforcement is left largely, if not wholly, in the hands of the patent holder. Intuitively, we know that digital technologies have somehow changed the nature of the game, especially in copyright, but we have yet to develop a coherent theory that specifies where the various lines should be drawn. We know that copying and worldwide distribution is easier, cheaper, and faster than was possible in the analog world, so the question is, or should be, how this easier, cheaper, and faster copying changes our feelings concerning who should be responsible for what in enforcing the private intellectual property rights held by content owners.

As the *Netcom* case shows, traditional principles of secondary liability do bring with them some added responsibilities, which is why the battle has been raging over what is meant by "actual knowledge" of the infringement to which one is accused of contributing. That approach seems unproblematic in cases like bulletin boards, at least once the operator of the service has actual notice of a specific infringing item. It becomes more problematic in cases like *Visa International*, where the paying financial institution has actual knowledge of the infringing activity in general and, at least arguably, makes a material contribution in effecting the money transfer between purchaser and infringer. However, as would be the case under SOPA, stopping all payments to the allegedly infringing site runs the risk of cutting off all transactions with that site, not just those that are the subject of the specific infringement complaint.

Further, traditional secondary liability does not generally reach at all the other objects of SOPA's regulation, namely, advertisers. It is difficult to argue that advertisers on a site that contains or offers infringing material make a material contribution to the infringe-

---

[117] These authors concede that applying their approach to conduit ISPs is considerably more complicated, as its application would involve inspecting huge amounts of internet traffic in real time and the absence of transparency, as a result of which the ISPs would be tempted to sacrifice user interests in the face of demands from rightowners. *Id*. at 1242. The authors do not attempt to apply their model to third parties like payment providers or web advertisers, but it seems that similar objections would apply in those realms, as well.

ment, or that they are in a position to control the actions of the infringer. So, we have moved from a relatively straightforward secondary liability problem for the web host in *Netcom* to giving power to intellectual property rightholders under SOPA to effect a change in otherwise entirely legal business relations between an advertiser and an allegedly infringing website. Had SOPA been enacted but proved with time to be less effective than hoped, it would be surprising if we did not hear demands for yet greater participation by third parties in copyright enforcement.

Many arguments against regulating, or at least against overregulating, ISPs and other third parties with respect to copyright infringement on the Internet fall into traditional balancing: content owner interest in intellectual property rights enforcement versus user interests in matters like privacy, free expression, loss of rights only after a hearing by an impartial judge, and transparency in regulatory processes. Section 512 of the U.S. Copyright Act and the EU E-Commerce Directive clearly represent a set of policy compromises among various players in the light of these policy considerations, as, indeed, did SOPA and ACTA. The question still remains, however, why we are involved in this kind of policy balancing at all: How did it become accepted that private third parties should be part of the copyright enforcement scheme?

It seems to come down to that favorite weasel word of the law, reasonableness. We have long demanded that people take reasonable care so that their otherwise legal actions do not harm others. The *Netcom* court itself looked to whether the defendant acted reasonably in response to the notice of infringing activity in determining whether the defendant made a material contribution to the infringement. While "acting reasonably" and "material contribution" do not have an obvious logical connection, the infringer in *Netcom* was using Netcom's facilities, at least arguably, with Netcom's knowledge. Requiring the ISP to "act reasonably" seemed like a perfectly natural extension of traditional concepts of contributory infringement. However, by what legal theory do we extend this reasoning to Internet advertisers as SOPA would have done? And does it make sense to extend it to credit card companies who participate in the payment transaction, as Judge Kozinsky would have done in the *Visa* case? Perhaps a general rule is evolving in which people simply must do what is reasonable when they have a degree of knowledge of an illegal act and are in a position to stop it. If we limit this new "rule" to intellectual property infringement, the question is, why only intellectual property rights? If we are expanding the obligations of people more generally, the question is, why are we not having a fuller discussion of this radical change in our legal thinking?