ISSN 1392-6195

JURISPRUDENCIJA
Mokslo darbai
2006 5(83); 9–19

LIABILITY OF INTERNET SERVICE PROVIDERS UNDER UNITED STATES LAW

Dennis S. Karjala

Jack E. Brown Professor of Law
Arizona State University
McAllister & Orange Streets, P.O. Box 877906, Tempe, Arizona
Phone: 85287-7906; 480-965-6181
E-mail: Dennis.Karjala@asu.edu

Pateikta 2006 m. vasario 6 d., parengta spausdinti 2006 m. gegužės 5 d.

Abstract. The ease with which copyright-protected material may be copied and distributed over the internet, and the difficulty of locating and sanctioning individual infringing end users, has focused much attention on the role of internet service providers (ISPs) in the enforcement of copyright rights. United States courts began assessing ISP liability for infringements by others making use of ISP facilities by applying common law notions of secondary liability, particularly contributory infringement, in an effort to strike an appropriate balance between enforcing copyright rights and allowing free use of a valuable new technology. In 1998 the U.S. Congress codified and amplified the general approach taken by the courts in section 512 of the Copyright Act, a complex provision that addresses in detail many of the fundamental issues. This article outlines these developments and analyzes the major cases that have interpreted the statutory provisions.

Keywords: internet service providers liability, copyright violations in cyberspace, contributory infringement of copyright.

1. INTRODUCTION

No one seriously doubts the potential of the internet to supply an important net social benefit by allowing the easy and inexpensive acquisition and distribution of information across the globe. On the other hand, many worry about the potential of the internet to undermine the creation incentives of copyright law by making the piracy of copyright-protected content not only cheap and easy but also very difficult to detect. Moreover, even when piracy has been detected, enforcement against any given actual infringer is cumbersome and damages likely to be only a small percentage of the total losses to piracy. Consequently, content providers have naturally sought ways to involve the internet service providers (ISPs) in their enforcement efforts.

Content providers would like the ISPs to police their networks much more carefully to find and stop infringing activity. Where the ISP has not made reasonable efforts to assist in enforcement, content providers often seek to hold the ISP liable for infringing activity that takes place on the ISP's network. The ISPs, on the other hand, do not like the idea of spending resources for the benefit of outsiders such as content owners and argue that they should not be held responsible for the infringing activities of their customers, any more than a telephone company should be held liable for, say, defamatory words published on a telephone network. The internet, they argue, is a device that can be used for an infinite variety of perfectly legal purposes, and infringing piracy is simply an unfortunate by-product of that advance in technology.

In the United States, first the courts and then Congress have stepped in to mediate this question of who should be held liable for infringing activity that takes place on the internet. The courts have tailored the common law notion of contributory infringement to meet some, but not all, of the content providers' demands. Congress, following the judicial lead, has acted through a relatively new provision of the Copyright Act, essentially to codify the judicial doctrines in statute, but with important amplifications and clarifications. This article attempts to analyze and explain these important developments.

2. THE BASIS FOR ISP LIABILITY

2.1. The RAM Copying Doctrine

Crucial to the analysis of ISP liability is the notion of RAM (random access memory) copying. Following the definition of "copy" in the Copyright Act [1], courts fairly early in the days since digital technologies came into widespread use concluded that causing a copyright-protected work to be stored in computer RAM involved the making of a "copy" [2], which means that the action is unlawful absent a license or some sort of defense.

ISPs perform a number of activities that potentially raise an infringement question under the RAM copying doctrine. At the most basic level, ISPs serve to connect computers that are operating on the internet, transmitting digital electronic signals according to their users' instructions. If a given transmission involves a copyright-protected work, the ISP not only makes it possible for users to make their own copies of the work but actually makes temporary copies itself as the material flows through the system. ISPs also provide searching services, which can require the ISP to make temporary copies of protected material at sites to which the ISP supplies links. In connection with searches, ISPs often find it technologically convenient to place stored material in "cache" so that the material can be retrieved more quickly when requested by users. Finally, ISPs may supply bulletin board services, with or without review or analysis of the content of the material that is posted on the bulletin boards. If the server housing the bulletin board belongs to the ISP, the ISP has arguably made a copy of the content contained there. Thus, the equipment of every ISP necessarily makes "copies" even of the works that flow through the ISP's system, because a copy will be at least temporarily stored in RAM somewhere in the system. It goes without saying that copies of works that are stored on hard drives or other nonvolatile memory within the ISP's system constitute "copies." The question is whether all this copying constitutes infringement when the copied work is protected by copyright.

2.2. Secondary Liability for Copyright Infringement

To the extent an ISP engages in actual copying of protected works (or in their distribution, public performance, or public display), it is a direct infringer of copyright absent a license or defense (such as fair use). However, United States law has long held people liable as copyright infringers even where they do not themselves engage in direct infringement. The two doctrines of relevance here are those of *contributory infringement* and *vicarious liability*.

A person may be liable as a contributory infringer if, with knowledge of the infringing activity, he materially contributes to the infringing conduct of another [3]. Thus, operation of Napster's centralized computer, which put Napster users in touch with one another so that they could exchange copyright-protected music files, made Napster a contributory infringer with respect to the direct infringement of its users [4]. Moreover, a person who has no actual knowledge of the infringing activity may still be liable vicariously if he has the right and ability to supervise the infringing activity and receives a direct financial benefit from it. Thus, the operator of a flea market who rents space to individual vendors to sell their wares may be liable if one such vendor sells pirated music, even if the flea market operator has no actual knowledge of the sales of pirated merchandise [5]. Both contributory infringement and vicarious liability have been major issues in the ISP cases.

There is an important limit on the contributory infringement doctrine: In *Sony Corp. of America v. Universal City Studios, Inc.* [6], the United States Supreme Court rejected a contributory infringement challenge to the manufacture and distribution of video cassette recorders. The movie studios argued that such devices allowed, indeed even encouraged, the making of infringing copies of their works that were broadcast on television.

Because the copying consumers were infringers, Sony was asserted to be a contributory infringer for distributing the means with which consumers could make the infringing copies. The Supreme Court held, however, that the video recording technology was capable of substantial noninfringing uses, such as taping programs whose copyright owners did not object or fair use taping of programs for later viewing at a more convenient time (after which the tape would be erased or covered over). The Court reasoned that Congress, not the courts, should determine how to balance the various interests of the copyright owners, on the one hand, and the public's desire to use a convenient new technology on the other. The *Sony* rule is, however, under challenge. The Supreme Court will hear in the spring of 2005 the case of *Metro-Goldwyn-Mayer Studios, Inc. v. Grokster, Ltd.,* [7] where distribution of a successor technology to that involved in Napster, which does not involve a centralized directory and therefore does not allow control over what files are transferred among users, is alleged to constitute contributory infringement.

2.3. The Netcom Case

Religious Technology Center v. Netcom On-Line Communication Services, Inc. [8] is the seminal case dealing with ISP copyright infringement liability. Netcom was an ISP that supplied internet connections to its clients. One such client was a person named Klemesrud, who operated a bulletin board service (BBS) at his home and connected to the internet through a Netcom account. About 500 people used Klemesrud's BBS to make postings available on the internet, including Erlich, who used the BBS to create a Usenet newsgroup for discussion and criticism of an organization known as the Church of Scientology. As part of that criticism, Erlich posted works in which the Church owned the copyright. The Church contacted both Klemesrud and Netcom, demanding the removal of Erlich's postings. Klemesrud

refused until the Church supplied proof that it owned the copyrights in question, and Netcom refused on the ground that it would be impossible to prescreen each of Erlich's postings and that to keep Erlich off completely Netcom would also be forced to cut off all of the other Klemesrud clients. Against Netcom, the Church asserted both direct and secondary liability.

On the issue of direct liability, the court agreed that a "copy" of the Church's works was made on both Klemesrud's and Netcom's computers whenever Erlich posted something to the BBS. It noted, however, that neither Netcom nor Klemesrud initiated the copying. Moreover, Netcom operated simply as a conduit, without monitoring messages that are posted or attempting to control the content of the information available through its system. The court concluded that storage on a server of material that has been uploaded by an infringing user is not a direct infringement of the exclusive right of reproduction. Otherwise ISPs all over the world would be infringers every time a customer posted an infringing copy on a bulletin board.

The *Netcom* court similarly held that Netcom did not infringe the exclusive rights of public distribution or display. Emphasizing that Netcom neither created 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 Usenet 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.

The Church also failed in its attempt to impose vicarious liability on Netcom. While the court, on a motion for summary judgment, concluded that there were genuine issues of material fact to be determined as to whether Netcom had the right and ability to control the activities of its users, it found that Netcom did not derive a direct financial benefit from the infringing activity because Netcom charged a fixed fee regardless of the nature of the content posted on its servers [9].

However, the court decided that a full trial on the merits was necessary on the Church's contributory infringement claim. Netcom did receive a notice from the Church along with a demand that Netcom stop the infringing activity, so at least as of that time Netcom was possibly in a position to stop the infringing activity. If it knew about the infringement (by Erlich) and failed to do anything about it, Netcom would be deemed to have substantially contributed to the infringement, thereby fulfilling both elements of a contributory infringement claim (knowledge and substantial participation) [10].

Congress used the *Netcom* case as the basis for a much more precise, and complex, amendment to the Copyright Act to cover ISP liability.

3. SECTION 512 OF THE COPYRIGHT ACT

Section 512 of the Copyright Act was adopted in 1998 as part of the so-called "Digital Millennium Copyright Act." Section 512 protects an ISP who meets the conditions of one or more of its four "safe harbors" from liability for monetary damages from 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.

Section 512 is a complex statutory provision, but its basic operation can be understood by breaking it down into its constituent pieces. It begins, in subsections 512(a), (b), (c), and (d), with the four safe harbors themselves, defining 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 provisions require the ISP to take affirmative action to disable access to or remove infringing material of which they are given notice, and section 512(g) permits ISPs to replace the material or reenable access 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 that ISPs implement a policy of terminating clients who are repeat infringers. A new notion in intellectual property enforcement has been created in section 512(h), which allows copyright owners, even though not yet parties to a lawsuit, to obtain a subpoena from the *clerk* (not a judge) of a U.S. federal district court requiring the ISP to disclose to the copyright owner information to identify the alleged infringer. Other provisions supplement this basic structure, some of which will be discussed as we proceed.

3.1. Types of ISPs

The safe harbor of section 512(a) applies to ISPs who might otherwise be deemed infringers by reason of "transmitting, routing, or providing connections for" infringing material through their systems or intermediate transient storage of such material. A 512(a) ISP is therefore one who performs a conduit role in connecting customers to the internet. Netcom appears to have been a 512(a) ISP. Section 512(b) immunizes eligible ISPs for practices involving "system caching," that is, the temporary storage of material within their systems for the purpose of more efficient operation, which involves saving all or a portion of the content of web sites for the purpose of delivering that content faster to subsequent users who request it. Section 512(c) applies to bulletin board systems, such as the one operated by Klemesrud in the *Netcom* case. It immunizes eligible ISPs from liability for the storage on their systems of infringing material

that is put there by someone else. Section 512(d) operates similarly to immunize eligible ISPs from liability for linking users to sites that may contain infringing material.

All of the safe harbors protect "service providers" who engage in the conduct specified in 512(a) - (d). The term "service provider" (i.e., ISP) is defined in section 512(k) in two ways. For purposes of section 512(a), a "'service provider' means an entity offering the transmission, routing, or providing of connections for digital online communications, between or among points specified by a user, of material of the user's choosing, without modification to the content of the material as sent or received" [11]. This definition tracks the language of 512(a) itself specifying the acts in which a 512(a) ISP may safely engage. For all other purposes, including of course sections 512(b) - (d), a "service provider" is more broadly defined as "a provider of online services or network access, or the operator of facilities therefor, and includes [a 512(a) ISP]" [12].

3.1.1. "Backbone" Services under Section 512(a)

Section 512(a) applies to ISPs who supply a connection to the internet. No monetary relief may be obtained against an ISP for copyright infringement "by reason of the [ISP]'s transmitting, routing, or providing connections for, material through a system or network controlled or operated by or for the service provider, or by reason of the intermediate and transient storage of that material in the course of such transmitting, routing, or providing connections," provided certain conditions are met: The transmission must be initiated by someone other than the ISP, everything must happen automatically without any selection by the ISP, the recipient is not selected by the ISP, no copies are maintained, and the material is transmitted without content modification [13]. These conditions are usually satisfied where the ISP does nothing more than supply an internet connection. Therefore, ISPs comprising the backbone of the internet by allowing customers to connect are generally eligible for this important safe harbor.

3.1.2. ISP Bulletin Board Services and the 512(c)(3) Notice

Section 512(c) immunizes ISPs from copyright infringement "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" [14]. The safe harbor is subject to the conditions that the ISP have no actual knowledge of the presence of infringing material, that the ISP is not aware of information from which "infringing activity is apparent," and that upon obtaining such knowledge or awareness the ISP acts "expeditiously" to remove or disable access to the infringing material. The safe harbor is further conditioned on the absence of any financial benefit to the ISP directly attributable to the infringing activity and, perhaps most importantly, upon receiving a statutorily specified form of notice from the copyright owner under section 512(c)(3), the ISP must respond "expeditiously" to remove or disable access to the infringing material [15]. Moreover, the ISP must designate an agent to receive 512(c)(3) notifications both on a web site available to the public and with the Copyright Office [16].

The requirements of the notification specified in section 512(c)(3) are set out in some detail in the statute. The substantive requirements, with which the notification must "substantially" comply, are identification of the work claimed to be infringed, or in the case of multiple works a representative list of infringed works at the site in question; identification of the material claimed to be infringing with information sufficient to allow the ISP to locate it; and a statement of good faith belief that the use complained of has not been authorized by the copyright owner. (Note that the notice does *not* have to specify even a good faith belief that the use is infringing – only that it has not been authorized.) A notice that "fails to comply substantially" with the requirements is not to be considered in determining whether an ISP otherwise has actual knowledge or the infringement or is aware of information making infringing activity apparent [17].

While we are discussing the 512(c)(3) notification, it is appropriate to discuss as well the "counter notification" made possible by section 512(g). This provision first exempts the ISP from liability for good faith removal or disabling activity relating to material claimed to be infringed, whether or not infringement is ultimately determined. This exemption, however, is itself conditioned on the ISP's notifying its customer that it has removed or disabled access and, upon receipt of a *counter notification* replaces the removed material or ceases disabling access to it after 10 days unless the copyright owner has brought an infringement action in court. The counter notification must include a statement of good faith belief that the material was removed or disabled as a result of mistake of misidentification [18]. With respect to both the notification and the counter notification, anyone who knowingly and materially misrepresents that material is infringing or was removed or disabled by mistake is liable for damages, including attorneys fees, incurred by those injured by the misrepresentation [19].

The intended operation of section 512(c) seem reasonably clear: An ISP whose customers run bulletin board systems using the ISP's storage and related facilities will not be liable, without more, simply because their customers post infringing material on a bulletin board. The ISP must take action, however, once it has actual knowledge of the presence of infringing material or is aware of facts that make infringing activity apparent. In particular, the ISP must respond expeditiously to a 512(c)(3) notification containing the statutorily required information by removing the allegedly infringing material or disabling access to it. If the customer believes that a mistake has been made, the customer can file a counter notification, in which case the ISP is required to replace the material unless the copyright owner brings a formal copyright infringement action in court. The ISP who complies with these requirements cannot be held

liable for damages from copyright infringement. Moreover, under section 512(m), none of the safe harbors in sections 512(a)-(d) may be conditioned on as ISP's "monitoring its service or affirmatively seeking facts indicating infringing activity" [20]. The statute thus expressly prohibits withholding safe harbor protection from ISPs who do not engage in their own detective work to uncover infringing activity in their systems.

3.1.3. System Caching by ISPs

Section 512(b) applies to ISPs who might otherwise be charged with copyright infringement "by reason of the intermediate and temporary storage of material on a system or network controlled or operated by or for the service provider," provided the material is made available by a third party, the material is transmitted by the third party to a requesting recipient, and the storage is governed by automatic technical processes. Section 512(b)(2) then sets some additional conditions designed to insure that caching does not result in the delivery of out-of-date information and does not subvert the conditions for entrance to the original site, such as payment of a fee.

Section 512(b)(5) adds a condition of a different type: Where the web site whose material is cached makes copyright-protected material available without authorization of the copyright owner, the ISP must respond "expeditiously" to remove or disable access to the material upon receiving a notice of the type specified in section 512(c)(3). Thus, the "notice and takedown" provisions applicable to bulletin board services under 512(c) apply as well to ISPs who engage in system caching.

3.1.4. Use of Information Location Tools

The fourth and final ISP safe harbor is found in section 512(d), which immunizes ISPs from copyright infringement "by reason of the provider referring or linking users to an online location containing infringing material or infringing activity, by using information location tools, including a directory, index, reference, pointer, or hypertext link." This provision seems aimed at protecting search services from companies like Yahoo and Google (but arguably even Napster might have qualified under this provision, as is discussed below). Again, as with bulletin board systems under 512(c), the 512(d) safe harbor is subject to the conditions that the ISP have no actual knowledge of the presence of infringing material, that the ISP is not aware of information from which "infringing activity is apparent," and that upon obtaining such knowledge or awareness the ISP acts "expeditiously" to remove or disable access to the infringing material. The safe harbor is further conditioned on the absence of any financial benefit to the ISP directly attributable to the infringing activity and upon receiving "a notification of claimed infringement as described in section 512(c)(3)," the ISP must respond "expeditiously" to remove or disable access to the infringing material.

3.2. Identification of Infringers

As part of the quid pro quo for exempting ISPs meeting the statutory conditions from copyright liability based on acts of their customers, Congress adopted a new and more streamlined provision for the issuance of subpoenas requiring ISPs to disclose information concerning their infringing customers. Normally subpoenas are issued in the course of litigation, as one of the parties discovers that information relevant to his case is known or held by another party or an outsider. Under section 512(h), however, a copyright owner who has not filed any infringement action may request a subpoena to an ISP for identification of an alleged infringer, and if relatively objective conditions are satisfied, the clerk of the court is required to issue it.

The copyright owner may request the subpoena by filing with the clerk a copy of the 512(c)(3) notification, a proposed subpoena, and a sworn declaration that the information obtained will be used solely for the purpose of protecting copyright rights [21]. If the notification satisfies the requirements of section 512(c)(3) and the accompanying materials are in order, the clerk "shall expeditiously issue" the subpoena requiring the ISP to disclose to the copyright owner information sufficient to identify the alleged infringer of the material described in the notification [22].

4. JUDICIAL INTERPRETATIONS

Although these ISP liability provisions have only been in effect for a few years, a number of courts have been called upon to interpret their meaning. We review here some of the more important judicial developments

4.1. Is Section 512 Exclusive?

In *CoStar Group, Inc. v. Loopnet, Inc.* [23], plaintiff CoStar argued that any immunity for passive ISP conduct must come solely from section 512, so that *Netcom* was to that extent superseded. In this case, the defendant Loopnet ran a web site permitting real estate brokers to post listings of commercial real estate that was for sale. The postings often included photographs. CoStar alleged that photos in which it owned the copyrights appeared at the Loopnet site, having been uploaded by Loopnet's clients. At the summary judgment stage, the lower court concluded that Loopnet was not eligible any of the section 512 safe harbors because there remained fact issues to be decided concerning whether Loopnet responded expeditiously to notifications of infringement and whether its termination policy was reasonable and effective [24]. However, when the claims were reduced by stipulation to one of direct infringement, the lower court ordered judgment for Loopnet, relying on *Netcom*. CoStar appealed, arguing that failure to comply with section 512 rendered Loopnet strictly liable under the Copyright Act.

The Fourth Circuit Court of Appeals agreed with *Netcom* that direct copyright liability required some-

thing more than mere ownership of a machine that was used by others to make copies. Rather, volitional conduct amounting to infringement is necessary to be held liable as a direct infringer. It then turned to CoStar's argument that section 512 superseded *Netcom*. The court noted section 512(l), which expressly states that failure to qualify under section 512 "shall not bear adversely" on any other defenses the ISP may have that conduct is not infringing. It also looked to statements in the legislative history that the section 512 was not intended to imply that an ISP was liable for conduct that failed to qualify under the statute for the safe harbor [25]. Given that section 512 was not exclusive, the court concluded that passively storing material at the direction of users to make the material available to others did not qualify as "making a copy" within the meaning of the Copyright Act [26]. In short, section 512 provides a *floor* of protection for ISPs, not a ceiling.

4.2. Qualification for the Safe harbors under Section 512

4.2.1. Section 512(a)

Perfect 10, Inc. v. CCBill, LLC, [27] involved several defendants who claimed the protection of section 512's safe harbors. Defendant IBill processes payments for online merchants but has no control over the content found at these merchants' sites. Because the infringing material did not go through IBill's site, Perfect 10 argued that IBill was ineligible for the 512(a) ISP safe harbor. But IBill did provide a connection to material on its clients' web sites through its system, so as to provide those clients with billing services. Consequently, it engaged in the behavior immunized by section 512(a): "providing connections for material through a system or network controlled" by the ISP. Therefore, IBill was a 512(a) ISP, eligible for the safe harbor protection if it met the other conditions of 512(a). Similarly, defendant CCBill supplied online accounting and statistical services to its web site clients, while also processing consumer payments by credit cards or checks. By providing a connection to material on its clients' web sites through its system, CCBill was entitled to the protection of the 512(a) safe harbor.

In the *Napster* litigation, Napster argued that it qualified for the safe harbor under section 512(a). As is well known, the Napster system operated via software that connected individual users' computers to the Napster central computer. Users seeking copies of music in mp3 format would log onto Napster, look for the music they wanted in the Napster directories, and click the appropriate buttons on their screens. The Napster computer then put the users seeking copies of music files into direct contact with users offering the music files in question and effected a download to the hard drive of the user seeking a copy of the music file. The district court agreed with Napster that (1) Napster did not initiate the transmissions, (2) the transmission was carried out automatically without selection by Napster, (3) Napster did not select the recipients, and (4) the material was transmitted without content modification. However, the court looked to the literal language of 512(a) and concluded that Napster did not "transmit[], rout[e], or provid[e] connections for, material *through* a system or network controlled or operated by" Napster [28].

This is very technical, probably result-oriented, reasoning, as it would not be difficult for a future Napster to route the downloads through the Napster computer. Liability for contributory infringement should not hinge on the details of the technologies that are involved but rather on economic substance. On appeal, the Ninth Circuit Court of Appeals questioned the trial court's conclusions on this issue, but elected to postpone detailed consideration of it until trial [29]. In any event, however, it seems likely that Napster would not have qualified for any of the safe harbors of section 512, because there was no evidence that the company had adopted or reasonably implemented a policy for dealing with repeat infringers under section 512(i).

4.2.2. Section 512(c)

The district court in *CoStar Group, Inc. v. Loopnet, Inc.* [30], considered whether Loopnet qualified as an ISP under section 512(c). It looked to the general definition of ISP in section 512(k) as "a provider of services or network access, or the operator of facilities therefore" [31]. CoStar argued that LoopNet was not a web page hosting service limited to the provision of Internet infrastructure, but the court concluded CoStar's definition was too limited. Loopnet was certainly engaged in providing online services, and that is enough to surmount the basic threshold of section 512(k)'s definition. While the court did not discuss it, it is also clear that Loopnet was storing material at the direction of its users on a system controlled by Loopnet, so the issue became whether Loopnet complied with the other requirements of section 512(c).

The district court in *CoStar* concluded that, while Loopnet employees were involved in the posting process, it was as a gateway (to try to stop the posting of infringing photos) and not as part of the selection process. The court concluded, "It would be inconsistent . . . if in order to get into the safe harbor, the provider needed to lack the control to remove or block access" [32]. Because Loopnet had received a valid 512(c)(3) notification, however, the court concluded that there were material issues of fact concerning whether Loopnet responded "expeditiously" to the notification and the adequacy of Loopnet's removal policy.

4.2.3. Section 512(d)

In the *Perfect 10* litigation [33], defendant Internet Key was a supplier of age verification services for "adult" web sites. Perfect 10 argued that Internet Key was ineligible for the 512(d) safe harbor, because, unlike Yahoo and Google, Internet Key did not use an "information location tool," such as a directory, index, reference, pointer, or hypertext link. Rather, Internet Key linked only to the small number of sites with which it had a contract. The court reasoned, however, that sec-

tion 512(d) refers to ISPs who refer or link to online locations containing infringing material. Internet Key used its own website, called "sexkey.com," to provide the reference or linking function, so it was at least eligible for the protection of 512(d) [34]. The court also concluded that statements by Internet Key clients that the photos were in the public domain or were posted for newsworthy purposes were insufficient to make the infringing activity "apparent" under 512(d)(1)(B) and that Internet Key had no right or ability to control the infringing activity.

The *Napster* case also involved arguments over whether Napster qualified for the safe harbor under section 512(d). Napster primarily relied on section 512(a) [35], presumably because 512(d) has more stringent requirements, in particular, the requirement of responding expeditiously to any notifications or actual knowledge of alleged infringement. But the 512(d) issue is also illuminating. Section 512(d) applies to service providers "referring or linking users to an online location containing infringing material or infringing activity, by using information location tools, including a directory, index, reference, pointer, or hypertext link." That, indeed, seems in substance to be exactly what the Napster system did. Napster argued that the information location aspects of its system were "incidental" to the core function of transmitting mp3 files, so that its safe harbor rights should be tested under 512(a). Napster attempted to distinguish its operations from those of a site like Yahoo, because Napster's operations were automatic once a user request was made whereas Yahoo's searches allegedly depended on human judgment and editorial discretion [36]. The court concluded that at least some of Napster's search and indexing functions were essential to the system's operation, so that those aspects should be tested under section 512(d) [37].

4.3. Implementation of a System for Termination of Repeat Infringers

Section 512(i), as discussed above [38], requires that ISPs adopt and reasonably implement a system for terminating repeat infringers in order to be eligible for any of the 512(a) - (d) safe harbors. Several cases have considered this requirement.

In *Corbis Corp. v. Amazon.com, Inc.* [39], the plaintiff asserted copyrights in pictures of celebrities that were being used without authorization on the pages of third-party vendors who displayed and marketed goods through Amazon's "zShops" service. Amazon claimed the protection of section 512(c), and Corbis argued that Amazon was ineligible for the safe harbor because it did not adopt or reasonably implement a system of termination of repeat offenders. Looking to a test devised by the Ninth Circuit Court of Appeals in an earlier case [40], the court found that 512(i) eligibility requires (1) adoption of a policy for termination of repeat offenders in appropriate circumstances, (2) informing users of the policy, and (3) reasonable implementation of the policy. Here Amazon's contracts with its zShops vendors prohibited copyright violations and stated that violations could result in termination, and that was sufficient to establish the existence of the required policy. Moreover, even though Amazon's policy did not disclose the criteria that would be used to determine who would be terminated, simply stating that "repeat infringement" would be sanctioned in appropriate circumstances was enough. The most important element of the test is reasonable implementation. The court concludes that the policy need not be perfect, only reasonable. Corbis's evidence that a once-cancelled vendor reappeared on Amazon under a different name does not, in itself, show failure to reasonably implement the policy. Moreover, even though Amazon did not terminate the accounts of two vendors after receiving messages from Corbis alleging infringement, these messages were insufficient to alert Amazon that they were engaged in blatant and widespread infringement. The court suggested the type of evidence that would make repeat infringement obvious: Statements at the site that pirated works were available or a discussion forum where customers exchanged views on how to get around copyright protections. Amazon was thus at least eligible for the 512(c) safe harbor insofar as the requirementsof section 512(i) were concerned [41].

Perfect 10, Inc. v. CCBill, LLC [42], involved several defendants who claimed the protection of section 512's safe harbors. Plaintiff Perfect 10 owns copyrights in a number of photographs that it claimed were infringed at the sites of these defendants' clients. All relied on the section 512 safe harbors as a defense to Perfect 10's infringement claims. Each of the defendants had a formal policy for termination of repeat infringers, so the issue was reasonable implementation.

In the case of IBill, Perfect 10 had submitted notifications under 512(c)(3), but they were deficient in failing to identify either the infringed photos or the URLs of the allegedly infringing photos. The court therefore refused to consider them as evidence of failure to implement IBill's repeat infringer policy [43], and Perfect 10's other evidence was insufficient to raise a material issue of fact concerning implementation. Perfect 10's purported notifications to CCBill and Internet Key also failed to comply substantially with the requirements of 512(c)(3), for similar reasons.

5. NON-DAMAGES ACTIONS AGAINST ISPS

5.1. Injunctive Relief

The safe harbors of sections 512(a) - (d) immunize ISPs from liability for monetary damages but expressly allow for limited injunctive or other equitable relief, as provided in section 512(j), for ISPs who are not subject to monetary damages, that is, those who qualify under one or more of the safe harbors. Again, the statute distinguishes between 512(a) ISPs, on the one hand, and 512(b) - (d) ISPs on the other.

For section 512(a) ISPs, injunctive relief is limited to an order to terminate the account of an identified cus-

tomer who is using the ISP's system to engage in infringing activity or an order requiring the ISP to take reasonable steps, specified in the order, to block access to a specific, identified, online location outside the United States [44]. For ISPs claiming the benefit of the other safe harbors in 512(b) - (d), an injunction may order the ISP to deny access to infringing material at a particular online site in the ISP's system, an order to terminate the account of an identified customer who is engaging in infringing activity, and "such other injunctive relief as the court may consider necessary to prevent or restrain infringement" of specified protected material at a particular online location, if such relief is less burdensome on the ISP than other forms of comparable relief. Coupled with section 512(m)(1), which expressly provides that the safe harbors may not be conditioned on the ISP's engaging affirmatively in monitoring users' activities for possible infringement, these provisions place the burden on the copyright owners to specify both the allegedly infringing users and the online location of infringing works before the qualifying ISP will be required to take action.

The injunction issued in the *Napster* case went well beyond the limits specified in section 512(j), in that it required very active searching and monitoring by Napster to root out infringing files listed on its directory [45]. The reason, as discussed above [46], is that the Ninth Circuit left resolution of the 512 safe harbors for trial, so it was not determined whether the limitations on injunctions would apply. We might question whether this delayed resolution of the availability of the safe harbors is consistent with the structure of section 512. There will nearly always be questions of fact over such things as implementation of repeat offender policies, whether an ISP was "aware" of circumstances making infringing activity apparent, or whether the ISP acted "expeditiously" in response to knowledge or notification of infringement. The approach of the Ninth Circuit in *Napster* allows all ISPs to be enjoined preliminarily and forces them to wait for a full trial to establish their right to protection under the safe harbors. One would think that at least a mini-trial of some sort should be required to determine whether a reasonable basis exists for assertion of safe-harbor protection. If Napster was, in fact, entitled to such protection, the company was out of business before it could take advantage of it.

5.2. Mandatory Disclosure of Customer Information

The new subpoena provisions under 512(h) have already been subject to an important judicial test. In *Recording Industry Association of America, Inc. v. Verizon Internet Services, Inc.* [47], the plaintiff RIAA got a subpoena ordering Verizon to disclose the names of certain Verizon subscribers who allegedly were trading large numbers of ".mp3" files using peer-to-peer sharing programs. Verizon refused, presumably seeking to establish or maintain a reputation for protecting the privacy of its customers, and the RIAA sued. Verizon argued in the district court that the new subpoena procedure applied only to 512(c) ISPs (those offering bulletin board services), because of the reference in the subpoena provision to the 512(c)(3) notification. The district court noted that sections 512(b) and (d), too, contained references to the 512(c)(3) notification and concluded that the subpoena provisions therefore extended beyond ISPs who supply bulletin board services. It also noted that P2P file sharing software was unknown when the DMCA was adopted in 1998 and that it was Congress's intent to permit the acquisition of customer information from ISPs in exchange for the limitation on ISP liability that section 512 affords. Therefore, it ordered Verizon to comply, even though Verizon was a 512(a) ISP [48].

The Court of Appeals, however, reversed. The court noted both the requirement for a copy of the notification to be filed with the request for subpoena and the close relationship between what a 512(b), (c), or (d) ISP receiving the notice could do in response to it. In contrast, 512(a) says nothing about a 512(c)(3) notification, because 512(a) ISPs act essentially as conduits for the information. Nothing is permanently stored on the system of a 512(a) ISP, and it makes no sense to talk about removing or disabling access to infringing materials of such an ISP's customers except in the extreme case of totally shutting off access to the internet by an accused customer. Consequently, the court concluded that the new subpoena provisions do not apply to 512(a) ISPs [49].

5.3. Notice-and-Takedown Provisions

We discussed above the "notice and takedown" provisions that are applicable to ISPs seeking to qualify for the safe harbors under sections 512(b) - (d) [50]. In *Online Policy Group v. Diebold* [51], the manufacturer of electronic voting machines was concerned about the availability on the internet of Diebold's internal email archive, which apparently included some statements by Diebold employees saying that the equipment did not always work right. Diebold sent cease and desist letters to the various ISPs involved, and at least one of them (Swarthmore College) complied by requiring students to remove the email archive from their campus website. The students and some of the ISPs sued Diebold, arguing under section 512(f) [52] that Diebold had "knowingly materially" misrepresented that posting the email archive online was infringing.

This is an interesting claim, because reproducing the emails certainly looks like a prima facie case of infringement. Diebold, as the employer, is considered the "author" of the emails under the U.S. "work made for hire" doctrine, and copying was clear. How could Diebold "knowingly" misrepresent that the actions of posting the email archive were infringing when, on the surface, they appear at least prima facie to be infringing? The court first found that, because the purpose of the posting was to inform the public about problems with Diebold's machines – a matter of crucial public interest and importance as such machines are used in many sta-

tes in the election of public officials – the posting was in fact a noninfringing fair use. But the court goes on to state that no reasonable copyright owner would have believed that the portions of the archive relating to problems with its voting machines were protected by copyright. Because Diebold knew that its cease-and-desist letters would affect the decision of the ISPs involved to take down the archive, which actually happened in some cases here, the misrepresentation was material and Diebold was liable under 512(f).

Note that the court in *Diebold* did not consider the students' rights under 512(g) to give a counter notification to get the email archive put back up. It would seem that the possibility of getting the material put back should at least have entered into the analysis of liability under 512(f). Fair use is a murky area, and close cases can almost never be resolved on summary judgment. The question is who should bear the burden of having to decide what is, or is not, a fair use. If a reasonable argument can be made on both sides, the statutory procedure essentially allows both parties to give their respective notifications, and the default position when that happens is that the material stays up and the ISP has no liability. Perhaps the *Diebold* court should have insisted that plaintiffs follow the counter notification procedure before filing their lawsuit. In any event, the case may indicate that the antimisrepresentation provisions of section 512(f) may have some real teeth.

CONCLUSIONS

The article outlined principal trends of the US statutory and case law on the internet service providers (ISPs). In the United States, first the courts and then Congress have stepped in to mediate this question of who should be held liable for infringing activity that takes place on the internet. The ease with which copyright-protected material may be copied and distributed over the internet, and the difficulty of locating and sanctioning individual infringing end users, has focused much attention on the role of internet service providers (ISPs) in the enforcement of copyright rights.

United States courts began assessing ISP liability for infringements by others making use of ISP facilities by applying common law notions of secondary liability, particularly contributory infringement, in an effort to strike an appropriate balance between enforcing copyright rights and allowing free use of a valuable new technology. In 1998 the U.S. Congress codified and amplified the general approach taken by the courts in section 512 of the Copyright Act, a complex provision that addresses in detail many of the fundamental issues, along with with important amplifications and clarifications of the case law.

Even further developments in the field remain to be crafted by the US Supreme Court in the case of *Metro-Goldwyn-Mayer Studios, Inc. v. Grokster, Ltd.*, which is expected to deliver new guidance for the ISPs and content owners.

REFERENCIES

1. 17 U.S.C.A. § 101 (definition of "copies"): "'Copies' are material objects, other than phonorecords, in which a work is fixed by any method now known or later developed, and from which the work can be perceived, reproduced, or otherwise communicated, either directly or with the aid of a machine or device."
2. MAI Systems Corp. v. Peak Computer, Inc., 991 F.2d 511. 9th Cir. 1993; Triad Systems Corp. v. Southeastern Express Co., 64 F.3d 1330. 9th Cir. 1995; Advanced Computer Services, Inc. v. MAI Systems Corp., 845 F.2d 356. E.D. Va. 1994.
3. *E.g.*, Fonovisa, Inc. v. Cherry Auction, Inc., 76 F.3d 259, 264. 9th Cir. 1996.
4. A&M Records, Inc. v. Napster, Inc., 239 F.3d 1004. 9th Cir. 2001.
5. Fonovisa, Inc. v. Cherry Auction, Inc., 76 F.3d 259. 9th Cir. 1996.
6. 464 U.S. 417. 1984.
7. 380 F.3d 1154. 9th Cir. 2004.
8. 907 F. Supp. 1361. N.D. Cal. 1995.
9. *Id.* at 1375-77.
10. *Id.* at 1373-75.
11. 17 U.S.C.A. § 512(k)(1)(A).
12. 17 U.S.C.A. § 512(k)(1)(B).
13. 17 U.S.C.A. § 512(a).
14. I discuss section 512(c) before 512(b) because the important provision for the contents of the notice required is contained in this provision. Its presence in section 512(c) and not as a more general condition to some or all of the safe harbors is likely an artifact of the legislative process rather than a considered decision by the statutory drafters. This placement, however, has already generated important litigation, which is discussed below. See *infra* text accompanying notes 47-48.
15. 17 U.S.C.A. § 512(c)(1).
16. 17 U.S.C.A. § 512(c)(2).
17. 17 U.S.C.A. § 512(c)(3)(B)(i). In *ALS Scan, Inc. v. Remarq Communities, Inc.*, 239 F.3d 619 (4th Cir. 2001), the plaintiff ALS owned the copyright in photographs that could be found on newsgroups accessible through the defendant ISP's service. Two such newsgroups – "alt.als" and "alt.binaries.pictures.erotica.als" – allegedly contained hundreds of postings that infringed plaintiff's copyrights. Plaintiff sent defendant Remarq a letter stating that these two sites "were created for the sole purpose" of infringing the plaintiff's copyrights and that virtually all the photos at those sites were infringing. Defendant, however, refused to cut off access, stating that it would eliminate any individual infringing items that plaintiff identified with sufficient specificity. Remarq defended against ALS's suit on the basis that it was immune from monetary liability under 512(c). Remarq argued that ALS had failed to identify the infringing works to which it was supposed to deny access, as required by 512(c)(3). ALS argued that it substantially complied with the notification requirement to specify the infringed works by stating that virtually all works at these specific newsgroups were infringing. The court noted that the statute permits the notification to contain merely a "representative list" of the infringed works and held that the notice ALS sent to Remarq was equivalent to such a representative list by specifying the two sites and stating that virtually all the photos at each were infringing copies. In addition, ALS's photos each included ALS's name and/or the copyright symbol next to it. Therefore, the court

concluded that the notice substantially complied with the requirements of 512(c)(3).

18. 17 U.S.C.A. § 512(g).
19. 17 U.S.C.A. § 512(f).
20. 17 U.S.C.A. § 512(m). The ISP can be required comply with standard technical measures used by copyright owners to identify and protect copyright-protected works. Such compliance, in addition to having a policy for terminating repeat infringers, is a general condition to the availability of each of the four safe harbors. 17 U.S.C.A. § 512(i).
21. 17 U.S.C.A. § 512(h)(2).
22. 17 U.S.C.A. § 512(h)(4).
23. 373 F.3d 544 (4th Cir. 2004).
24. Costar Group Inc. v. Loopnet, Inc., 164 F. Supp. 2d 688 (D. Md. 2001).
25. H.R. Conf. Rep. No. 105-796, at 73 (1998); *see* 373 F.3d at 553.
26. CoStar also argued that Loopnet's conduct was not wholly "passive," because Loopnet employees did attempt to screen photographs that were posted, in an effort to respond to CoStar's complaints about copyright violations. Quite sensibly, the court saw the perverseness of penalizing Loopnet for conduct intended to assist CoStar and others in enforcing their copyright rights, even though this reasoning has little logical bearing on the issue of whether Loopnet's conduct was passive. A dissenting judge concluded that Loopnet's activities were "anything but automatic" and would have found Loopnet liable. 373 F.3d at 560-61.
27. 340 F. Supp. 2d 1077. C.D. Cal. 2004.
28. [A&M Records, Inc. v. Napster, Inc., 2000 WL 573136, *7. N.D. Cal. 2000. (emphasis added).
29. A&M Records, Inc. v. Napster, Inc., 239 F.3d 1004 (9th Cir. 2001). Of course, the trial was never held, as Napster went out of business shortly after the Ninth Circuit decision. We discuss below whether the Ninth Circuit was correct in postponing resolution of this issue. See *infra* text accompanying notes 45-46.
30. 164 F. Supp. 2d 688. D. Md. 2001; see *supra* text accompanying notes 23-26.
31. 17 U.S.C.A. § 512(k)(1)(B). This is the definition that applies for purposes of sections 512(b)-(d). Section 512(a) ISPs are defined more narrowly: "an entity offering the transmission, routing, or providing of connections for digital online communications, between or among points specified by a user, of material of the user's choosing, without modification to the content of the material as sent or received." 17 U.S.C.A. § 512(k)(1)(A).
32. 164 F. Supp. 2d at 702.
33. See *supra* text accompanying note 19.
34. When a user tries to go to one of Internet Key's clients, the user is directed to Internet Key to qualify for age verification. This is not covered by section 512(d), because Internet Key is not referring the user anywhere. However, the court concluded that this aspect of the operation was covered by 512(a), because Internet key is providing a connection to the material on its clients' web sites through its age verification system. 340 F. Supp. 2d at 1098-99.
35. See *supra* text accompanying note 28.
36. A&M Records, Inc. v. Napster, Inc., 2000 WL 573136, *5. N.D. Cal. 2000.
37. The court did not attempt the resolve the application of 512(d) to the Napster case, because in moving for summary judgment Napster did not rely on section 512(d). *Id.* at *6.
38. See *supra* note 20.
39. No. CV03-1415L, W.D. Wa., 21 Dec. 2004, available at http://pub.bna.com/ptcj/031415orderDec21.pdf.
40. Ellison v. Robertson, 357 F.3d 1072. 9th Cir. 2004.
41. On the merits, Corbis did not give Amazon a 512(c)(3) notification, so its claim was based on the more general rules of 512(c) concerning whether Amazon had actual knowledge of the infringing activity or was aware of facts or circumstances from which infringing activity was apparent. Corbis supplied no evidence that Amazon had actual knowledge of infringements of Corbis's photos. As for awareness of apparent infringing activity, the court looked to the congressional history and concluded that apparent knowledge in this provision meant willfully turning a blind eye to red flags of obvious infringement. Corbis made no showing of such willful ignorance here. Consequently, Amazon was entitled to the protection of the 512(c) safe harbor.
42. 340 F. Supp. 2d 1077 (C.D. Cal. 2004); see *supra* text accompany note 27.
43. Section 512(c)(3)(B)(i) provides that a notification that fails to comply substantially with section 512(c)(3)(A)'s requirements shall not be considered in determining whether the ISP has actual knowledge or awareness sufficient to deny the protection of the 512(c) safe harbor.
44. 17 U.S.C.A. § 512(j)(1)(B).
45. The Ninth Circuit placed the burden on the recording companies to provide notice to Napster of infringed works and files containing them on the Napster system before Napster had the duty to disable access to the offending content. It said, however that "Napster . . . also bears the burden of policing the system within the limits of the system." A&M Records, Inc. v. Napster, Inc., 239 F.3d 1004, 1027. 9th Cir. 2001.
46. See *supra* text accompanying note 29.
47. 351 F.3d 1229. D.C. Cir. 2003.
48. *In re* Verizon Internet Services, Inc., 240 F. Supp. 2d 24. D.D.C. 2003.
49. In this context it might be noted that Germany, too, has come to a similar conclusion concerning an ISP's obligation to reveal the names of its customers, although on different reasoning. German law permits a copyright owner to demand information from an infringing party on the source of illegal copies, but here the ISP was not an infringer because, absent knowledge of the infringing activity, it neither committed nor participated in the violation. The court did note, however, that German law freeing ISPs from the obligation to monitor content does require ISPs to act once they have knowledge of user violations. OLG Frankfurt, No. l 11 U 51/04, 25 Jan. 2005 (Franklin am Main High Regional Court), *summarized at* 10 BNA Electronic Commerce &Law Reports, No. 5 (2/2/05), http://pubs.bna.com/ip/BNA/eip.nsf/is/a0b0h8h5t6.
50. See *supra* text accompanying notes 15-18.
51. 337 F. Supp. 2d 1195. N.D. Cal. 2004.
52. See *supra* text accompanying note.

INTERNETO PASLAUGŲ TEIKĖJO ATSAKOMYBĖ PAGAL JAV TEISĘ

Dennis S. Karjala
Jacko E. Browno vardo profesorius
Arizonos valstijos universitetas, JAV

S a n t r a u k a

Straipsnyje nagrinėjami JAV intelektinės nuosavybės naudojimą ir atsakomybę už intelektinės nuosavybės pažeidimus nustatantys teisės aktai ir svarbiausi teisiniai precedentai. Daugiausia dėmesio straipsnyje skiriama JAV interneto paslaugų teikėjų teisinės atsakomybės nustatymo reikalavimams. Straipsnyje apžvelgiamos pagrindinės interneto paslaugų teikėjų atsakomybės doktrinos, taikomos JAV, ir pateikiami jų teisminio interpretavimo komentarai.

XX a. pabaigoje JAV teismai suformulavo tris pagrindines interneto paslaugų teikėjų teisinės atsakomybės nustatymo doktrinas: *The RAM copying doctrine, Secondary liability for copyright infringement ir The Netcom case doctrine*. Šios doktrinos naudojamos sprendžiant interneto paslaugų teikėjų teisinės atsakomybės klausimus JAV.

Remdamasis JAV teisinėje praktikoje suformuotais teismų precedentais dėl intelektinės nuosavybės teisinės apsaugos internete, JAV Kongresas 1998 metais nustatė ir įdiegė teisinius reikalavimus interneto paslaugų teikėjams *U.S. Copyright Act* (Autorių teisių akte). Autorių teisių aktas numato interneto paslaugų teikėjų tipus, veiklos bei jos ribojimo teisines nuostatas ir reikalavimus teisinei atsakomybei nustatyti.

Svarbiausios JAV bylos, susijusios su Autorių teisių akto įgyvendinimu, yra *Corbis Corp. v. Amazon.com, Inc. ir Perfect 10, Inc. v. CCBill, LLC.* Minėtų bylų teismo sprendimai detalizavo Autorių teisių akto taikymo specifiką vertinant interneto paslaugų teikėjų teisinę atsakomybę.

Autorių teisių aktas taip pat numato teisinius reikalavimus, kuriuos įvykdęs interneto paslaugų teikėjas negali būti traukiamas teisinėn atsakomybėn. Pagal minėtą teisės aktą yra du pagrindiniai reikalavimai: interneto paslaugų vartotojo tapatybės atskleidimas gavus teismo šaukimą arba neteisėtai paskelbtos intelektinės nuosavybės pašalinimas iš interneto paslaugų teikėjų tarnybinių stočių.

Straipsnį sudaro šešios dalys: įvadas; interneto paslaugų teikėjų teisinės atsakomybės kvalifikavimo pagrindiniai reikalavimai; Autorių teisių akto nuostatos; teisminė interpretacija; interneto paslaugų teikėjų teisinę atsakomybę šalinantys reikalavimai ir išvados.

Pagrindinės sąvokos: interneto paslaugų teikėjų atsakomybė, autorių teisių ir gretutinių teisių pažeidimai elektroninėje erdvėje, netiesioginiai autorių teisių ir gretutinių teisių pažeidimai.