No. 03-1911

IN THE
UNITED STATES COURT OF APPEALS
FOR THE FOURTH CIRCUIT

COSTAR GROUP, INC. AND
COSTAR REALTY INFORMATION, INC.,

Plaintiffs-Appellants,

v.

LOOPNET INC.,

Defendant-Appellee.

On Appeal from the United States District Court
for the District of Maryland

BRIEF OF APPELLANTS

WALTER DELLINGER
JONATHAN D. HACKER
O'MELVENY & MYERS LLP
1625 Eye Street, N.W.
Washington, D.C. 20006
(202) 383-5300

Counsel for Appellants

CORPORATE DISCLOSURE

TABLE OF CONTENTS

Page

TABLE OF AUTHORITIES

Page(s)

CASES

TABLE OF AUTHORITIES (cont.)

Page(s)

STATUTES AND CONSTITUTIONAL PROVISIONS

LEGISLATIVE HISTORY

OTHER AUTHORITIES

INTRODUCTION

This case is another in a recent, well-publicized line of cases implicating the intersection of copyright law and the Internet.

The district court in this case summarily dismissed the direct copyright infringement claim of plaintiffs-appellants CoStar Group, Inc. and CoStar Realty Information, Inc. (collectively "CoStar"), against defendant-appellee LoopNet Inc. ("LoopNet"), on the ground that LoopNet, as an assertedly "passive" provider of Internet access and hosting services, is entitled to a categorical and conclusive immunity from direct copyright infringement claims based on material posted on LoopNet's website. The court derived this categorical immunity from *Religious Technology Center v. Netcom On-Line Communications Services, Inc.*, 907 F. Supp. 1361 (N.D. Cal. 1995), which had devised a special new rule of copyright infringement applicable to actions against Internet service providers ("ISPs"): if the ISP provides only "passive" services, the ISP cannot be held liable for direct infringement as a matter of law. This special immunity was based on the *Netcom* court's concern that, if traditional direct infringement principles are applied literally to ISPs, copyright liability could be spread through the Internet as fast as data can flow from one computer to the next.

Not long after the *Netcom* court devised its own unique solution to the problem of potentially limitless copyright liability for ISPs, Congress addressed the

very same problem in the 1998 Digital Millenium Copyright Act ("DMCA"). Congress's solution to the policy problem addressed in *Netcom* was *not* a categorical bar to certain claims against passive ISPs, but instead a "safe harbor" immunity from liability for which any ISP can qualify *if it meets certain conditions* – conditions that ensure that any ISP that cannot fairly be held responsible for material it distributes or displays will not be subjected to infringement liability. The necessary implication of the DMCA's structure is that if the ISP does *not* qualify for the statutory safe harbor, it is not within the category of ISPs that Congress deemed qualified for special, policy-based protections.

It is undisputed that LoopNet does not qualify for the DMCA safe harbor as to many of the infringing photographs displayed on its website. CoStar therefore should have been able to proceed with its claims of direct infringement as to those photographs. But the district court did not allow those claims to proceed. Rather than evaluate the factual record or legal analysis supporting those claims, the court held them barred at the threshold, on the basis of the special ISP-protecting rule proposed by the district judge in *Netcom*.

The question thus presented is whether an ISP that does not qualify for the legislatively prescribed immunity from direct infringement liability can nevertheless seek shelter in a more sweeping, judge-made immunity from the same liability. This Court answered that question squarely in the negative in *ALS Scan*,

Inc. v. RemarQ Communities, Inc., 239 F.3d 619 (4th Cir. 2001), which holds that an ISP's defense to liability under the principles of *Netcom* must be evaluated exclusively under the terms of the DMCA, *id.* at 622.

As *ALS Scan* recognizes, Congress addressed and resolved in the DMCA the new problems of potentially expansive copyright liability presented in the early Internet era. The DMCA gives courts a scalpel with which to carve out an immunity from infringement claims for *specifically qualified* ISPs. By contrast, the *Netcom* rule – followed by just a handful of courts prior to Congress's entry into the field – was a bludgeon that allowed courts simply to wipe out all direct infringement claims against any ISP deemed by the court to be "passive." The bludgeon approach may well have made sense in the early days of the Internet, when the threat of endless copyright liability was real. But that was before Congress – the entity with exclusive power under the Constitution to make the laws governing copyrights, U.S. Const. art. I § 8, cl. 8 – took convincing steps in the DMCA to confront and mitigate that threat, while still respecting and protecting the rights of copyright owners to prevent unauthorized uses and displays of their works in the digital environment. Judicial application of *Netcom* immunity to an ISP that does not qualify for the DMCA's more nuanced version of *Netcom* immunity contradicts and undermines that careful statutory balance. Accordingly,

the decision of the court below to grant LoopNet a categorical *Netcom* immunity from direct infringement claims is incorrect and should be reversed.

JURISDICTIONAL STATEMENT

This action arises under the federal Copyright Act of 1976, 17 U.S.C. §§ 101 et seq.; accordingly, the district court had exclusive jurisdiction pursuant to 28 U.S.C. § 1331 & 1338(a). On June 23, 2003, the district court issued a final order entering judgment against CoStar on its claim of direct infringement, and dismissing all other claims pursuant to joint stipulation of the parties. CoStar filed a timely notice of appeal on July 22, 2003. This Court has jurisdiction pursuant to 28 U.S.C. § 1291.

STATEMENT OF ISSUES

1. Whether the district court erred in granting LoopNet summary judgment on CoStar's claim of direct infringement solely on the basis of *Religious Technology Center v. Netcom On-Line Communications Services, Inc.*, 907 F. Supp. 1361 (N.D. Cal. 1995), a pre-DMCA decision holding that a "passive" Internet service provider is categorically immune from direct infringement claims, regardless of their underlying merit.

2. Assuming *Netcom*'s categorical bar to direct infringement claims against "passive" ISPs remains viable after the enactment of the DMCA, whether such a

bar applies to LoopNet, which engages in a personal, human review and approval of each and every photograph before it is displayed on LoopNet's website.

STATEMENT OF THE CASE

This appeal arises out of an action by CoStar against LoopNet for direct and contributory copyright infringement, violation of the federal Lanham Act, and various pendent state-law causes of action. CoStar filed the action in September 1999, after it discovered that scores, and eventually hundreds, of CoStar's copyrighted photographs were displayed on LoopNet's commercial website, and after LoopNet refused or failed to remove them after several requests. On December 8, 1999, LoopNet for the first time appointed an agent to receive notifications of potential infringements, as ISPs are required to do before they can assert immunity from copyright liability under the DMCA. JA29 n.4.[1] LoopNet subsequently claimed DMCA immunity for all infringing displays after December 8, 1999, but admitted that it did not qualify for immunity under the statute for any displays prior to that date. *Id.*

On March 14, 2000, the district court issued a preliminary injunction requiring LoopNet to remove all photographs as to which it had received infringement notifications from CoStar and to take certain steps preventing repeat infringements by LoopNet's users. Because CoStar continued to find infringing

[1] Material included in the Joint Appendix is cited "JA." Material cited from the record below is identified by its district court docket number, *e.g.*, Doc. 71.

photographs displayed on LoopNet's website despite these measures, CoStar subsequently sought modifications of the preliminary injunction that would expand its requirements to further prevent infringing displays. At the same time the parties were briefing the motion to modify the injunction, they were briefing cross-motions for summary judgment.

On September 28, 2001, the district court issued a consolidated opinion and order addressing the cross-motions for summary judgment and the motion to modify the injunction. *See CoStar Group, Inc. v. LoopNet, Inc.*, 164 F. Supp. 2d 688 (D. Md. 2001), *reprinted at* JA22-43. The court first granted LoopNet summary judgment on CoStar's claim for direct infringement. The court did not review the summary judgment record or otherwise analyze the existence *vel non* of material factual and legal disputes concerning the underlying claim. Instead the court dismissed the direct infringement claim at the threshold, relying exclusively on the rule barring direct infringement claims against "passive" ISPs set forth in *Religious Technology Center v. Netcom On-Line Communications Services, Inc.*, 907 F. Supp. 1361 (N.D. Cal. 1995). JA27-28. Under *Netcom*, the court held, the only type of copyright infringement claim that may be stated against a "passive" ISP is a claim for contributory infringement. *Id.*

Turning then to CoStar's contributory infringement claim, the court started by analyzing LoopNet's asserted DMCA immunity defense. The court held that

LoopNet was not entitled to summary judgment on this defense, because numerous material factual issues existed as to whether LoopNet had properly disabled access to certain infringing photographs and whether LoopNet had designed an adequate prevention policy with respect to certain users. JA33. The court also held that because LoopNet did not even assert DMCA immunity as to photographs displayed on its site prior to December 8, 1999, it could not claim DMCA immunity for any displays prior to that date. JA29 n.4.

Having rejected Loopnet's claim to summary judgment on the DMCA defense, the court turned to the underlying merits of CoStar's contributory infringement claim. That claim, unlike direct infringement, required proof that the defendant *knew* or *should have known* that the conduct it was facilitating was infringing. The court declined to grant either party summary judgment, because "too many material factual disputes" remained as to the level of LoopNet's knowledge with respect to each of the hundreds of infringing displays at issue. JA36.

The court also addressed several other substantive claims and defenses not at issue here. It rejected LoopNet's arguments that the licenses signed by CoStar's users allowed the photographs to be displayed on Loopnet's website and that CoStar had "misused" its copyright. JA26, 36-37. The court dismissed CoStar's pendent state-law claims as preempted by the Copyright Act, JA40-42, but rejected

LoopNet's similar preemption-based motion to dismiss CoStar's Lanham Act claim, JA40.

The court also denied in part CoStar's motion to modify the preliminary injunction, but did modify the injunction to enhance the extent to which LoopNet was required to police the activities of users who LoopNet knew had already submitted infringing photographs. JA42. CoStar took an immediate appeal from the denial of its broader request, but voluntarily withdrew that appeal on January 17, 2002.

On June 19, 2003, the parties filed a joint stipulation of dismissal of all claims except the direct infringement claim, clearing the way for the court to enter an order of final judgment in the case. The court did so on June 23, 2003, entering judgment in favor of LoopNet on CoStar's claim for direct infringement, and dismissing all other claims with prejudice as per the joint stipulation. JA21. On July 22, 2003, CoStar noticed its appeal with respect to the judgment on direct infringement.

STATEMENT OF FACTS

1. CoStar is "a national provider of commercial real estate information services." JA24. CoStar offers commercial real estate professionals and related businesses access to the most accurate and comprehensive databases of information on the U.S. and U.K. commercial real estate markets, and the largest

known digital image library of commercial properties.[2] Fifteen years ago the commercial real estate market was characterized by dispersed, fragmented and incomplete information, creating obstacles to efficient transactions. CoStar's proprietary databases have responded to that problem, collecting, developing and integrating a wide range of information, including information on leasing, sales, comparable sales, tenants, and digital photographs. These databases provide customers with critical information to understand market conditions, identify opportunities, value properties, and complete transactions efficiently.

CoStar's databases have been and continue to be built as a result of extraordinary effort and investment by CoStar. Over the past decade CoStar has invested literally hundreds of millions of dollars to develop not only sophisticated technology, but also highly qualified human resources, to provide and maintain database content. CoStar employs over 500 commercial real estate professionals, who collect and analyze commercial real estate information through millions of phone calls, emails, Internet updates and faxes each year, in addition to field inspections, public records review, news monitoring and direct mail. CoStar also has an extensive field research staff that physically inspects and photographs properties. JA50-51. This staff includes highly trained professional photographers. JA50.

[2] The following general background on CoStar can be found at www.costar.com.

Most of the property listings in CoStar's databases include photographs of the individual properties. JA2. These photographs are a critical component of the information CoStar makes available to its subscribers. JA46, 51. CoStar instructs its photographers which properties to shoot and defines the parameters for each shoot. JA50. Only those photographs that meet CoStar's quality criteria are used in the database. JA51. CoStar owns the copyright in the vast majority of photographs in its databases, and in all the photographs at issue here. JA48.

CoStar makes its databases available to its customers through CD-ROM and the Internet. JA46. Each of CoStar's customers signs a written agreement that explicitly prohibits the customer from posting CoStar's photographs on the website of the customer or of any third party. JA47.

2. LoopNet also provides commercial real estate information, in direct competition with CoStar, but through a different business model. Whereas CoStar employs its own researchers and photographers to build its information database, LoopNet obtains the information it provides on its website from its own users. And rather than obtain subscriptions for its services, LoopNet (at the time this lawsuit was filed and for most of the time it was pending below) generated income primarily by selling advertising on its website in the areas traveled by users seeking real estate information. Accordingly, LoopNet's business model depended on the submission of information and photographs by its users to attract other

users, who would then view the paid advertising. JA81, 87, 127-28. To that end, LoopNet actively encouraged its users submit material to its website, including photographs. JA95 (LoopNet submission form: "For optimal results on the Internet, include as much information as possible on your listing, particularly graphics."), JA149, 165.

The information users may submit is strictly controlled. LoopNet users may only submit information pertaining to commercial real estate, and they may do so only through a specific electronic form provided by LoopNet. JA25, 95-97. The form includes fields requiring identification of the property name, type, address, square footage, age, description, identifying information, and password. JA95-97. Once that form is submitted the property is added to LoopNet's database and listed on its website. JA25, 88.

Photographs are handled differently. If a user submits a photograph, it is diverted into a separate electronic folder elsewhere in LoopNet's system. JA25, 91-92. Each and every photograph submitted is then reviewed by a LoopNet employee. JA25, 67, 83, 89, 152. The employee examines the photograph for a number of purposes:

- To ensure that it is actually a photograph of commercial real estate. JA89, 152.
- To ensure that it does not contain an obvious copyright notice. JA67, 83, 157.

- To ensure that it does not include any logos or advertisements, for which LoopNet charges a separate fee. Doc. 94, Exh. F.

- To ensure that it is of adequate quality for posting. *Id.* When it is blurred or otherwise of poor quality, a LoopNet employee will sometimes edit the photograph to "clean it up" for the user. *Id.*

Collectively these requirements operate to ensure that only photographs that adhere to LoopNet's commercial mission are posted on its website. If the photograph does not satisfy all these requirements, the employee rejects the photograph and it is not posted to Loopnet's website. JA84. But if the employee deems the photograph to be satisfactory, the employee "accepts" the photograph and it is moved to a folder that allows for viewing on the website. JA25, 89, 183, 172.

3. In early 1998, CoStar became aware that its copyrighted photographs were appearing on LoopNet's website. CoStar informed LoopNet and identified the photographs, which LoopNet removed. JA70-74. But the pattern continued. In early summer 1999, CoStar discovered more than 20 copies of CoStar's photographs – from the D.C. market alone – displayed on LoopNet's website. JA55-56. By late summer CoStar had found a total of 112. *Id.* By the time the district court entered its opinion dismissing the direct infringement claims, CoStar had discovered more than 300 of its photographs copied, distributed, and displayed on LoopNet's website, JA25, and hundreds more were identified during the pendency of the proceedings below. Each time CoStar discovered additional infringing photographs, it informed LoopNet, which removed them, but not always

immediately, and not always permanently. The district court concluded that "[t]here are several material factual disputes . . . as to whether the removal of allegedly infringing photographs was satisfactorily expeditious and whether LoopNet's termination policy was reasonable and effective." JA33.

SUMMARY OF ARGUMENT

For two distinct reasons, the court's application of the *Netcom* rule to dismiss CoStar's direct infringement claims, without further analysis of those claims under standard copyright principles, was error.

First, this Court has already squarely held that "the policy-based protections articulated in *Netcom*," as LoopNet itself describes them, *see* Doc. 107, at 3, were "codified" by Congress into specific, statutory affirmative defenses under the DMCA. *See ALS Scan, Inc. v. RemarQ Communities, Inc.*, 239 F.3d 619, 622-26 (4th Cir. 2001). After the DMCA's "codification of the *Netcom* principles," this Court explicitly recognized, *Netcom* itself no longer imposes its own *independent* policy-based immunity on "passive" ISPs. *Id.* at 622. Rather, an ISP's *Netcom*-like special protection resides *exclusively* in the DMCA safe harbor. *Id.* Accordingly, if an ISP does not meet the statutory requirements for that protection, a court should not "double count" *Netcom* and thus provide the ISP an independent measure of special, judge-made immunity.

In this case the district court specifically held – and it is undisputed – that Loopnet does not qualify for DMCA immunity for a large subset of CoStar's direct infringement claims. JA29 n.4. The district court further held that material factual issues exist as to LoopNet's entitlement to DMCA immunity with respect to all remaining claims. JA33. The court therefore erred in granting summary judgment to LoopNet on the basis of any immunity from direct infringement claims. Because LoopNet has no valid defense to liability absent DMCA immunity, judgment should have been entered for CoStar on the direct infringement claims for which LoopNet indisputably does not qualify for such immunity, and further factfinding should have been undertaken with respect to the remaining direct infringement claims.

Second, even if it were appropriate to apply *Netcom* immunity to an ISP that failed to qualify for DMCA immunity, it would be improper to apply *Netcom* to LoopNet. LoopNet is not a "passive," "automatic" purveyor of electronic information of the kind involved and contemplated in *Netcom*. Rather, LoopNet strictly controls the content of all information submitted to its website – nothing other than real estate information is allowed, and that information is provided only on a specific form provided by LoopNet. Most important, a LoopNet employee reviews and approves every single photograph for consistency with LoopNet's commercial theme before the employee moves it into a folder for viewing on

LoopNet's website. Adhering to traditional principles of copyright liability under those circumstances would in no way threaten the very existence of the Internet – the policy concern underlying *Netcom* – because LoopNet differs so dramatically from those bulletin board services ("BBSs") and ISPs whose main function is simply to facilitate access and to handle data transfer in a truly neutral, automatic fashion. This case is indistinguishable from *Playboy Enterprises, Inc. v. Russ Hardenburgh, Inc.*, 982 F. Supp. 503 (N.D. Ohio 1997), a pre-DMCA case in which the court denied an ISP *Netcom* immunity where, as here, the ISP (1) encouraged the posting of material, and (2) screened all postings before moving them to a file for viewing. *Id.* at 513. Because *Netcom* thus does not apply here even by it own terms, it provides no basis for the district court's summary dismissal of the direct infringement claim.

ARGUMENT

The district court in this case granted LoopNet summary judgment on CoStar's claim of direct infringement for one reason, and one reason only: the district court chose to follow the rule enunciated by the trial court in *Netcom* that an ISP that provides only "passive" or "automatic" Internet services is categorically immune from direct copyright infringement claims based on material posted or displayed by the ISP's users. Holding that *Netcom*'s special new protective rule for "passive" ISP defendants categorically barred CoStar's direct

infringement claim, the court dismissed the claim without further analysis of LoopNet's liability for direct infringement under traditional copyright infringement principles. For the two reasons elaborated below, this ruling was erroneous, and should be reversed. Because this is an appeal from a grant of summary judgment in LoopNet's favor, this Court reviews the district court's order de novo, granting CoStar the benefit of all reasonable inferences from the factual record. *See Continental Airlines, Inc. v. United Airlines, Inc.*, 277 F.3d 499, 508 (4th Cir. 2002).

I. SUMMARY JUDGMENT ON DIRECT INFRINGEMENT SHOULD BE REVERSED BECAUSE LOOPNET DOES NOT QUALIFY FOR THE DMCA'S *NETCOM* SAFE HARBOR AND THERE IS NO BASIS IN LAW FOR IMPOSING AN INDEPENDENT, CATEGORICAL BAR TO DIRECT INFRINGEMENT CLAIMS AGAINST "PASSIVE" ISPs

A. *Netcom* Was A Policy-Based, Special Rule Of Protection From Copyright Liability For ISPs

1. "Reduced to most fundamental terms, there are only two elements necessary to the plaintiff's case in an infringement action: ownership of the copyright by the plaintiff and copying [or public distribution or public display] by the defendant." Melville B. Nimmer & David Nimmer, *Nimmer on Copyright* § 13.01, at 13-5 (2003); *see Keeler Brass Co. v. Continental Brass Co.*, 862 F.2d 1063, 1065 (4th Cir. 1988). Under traditional copyright principles, direct infringement is a "strict liability" claim: if the defendant displays the plaintiff's

copyrighted photograph, the defendant is liable (absent a statutory affirmative defense such as "fair use"), regardless whether the defendant knew or should have known that the photograph was copyrighted. *See Fitzgerald Pub. Co. v. Baylor Pub. Co.*, 807 F.2d 1110, 1113 (2d Cir. 1986); *Nimmer on Copyright* § 13.08, at 13-284.[3] The *Nimmer* treatise explains why even "innocent" infringers are held liable under traditional copyright rules:

> Copyright would lose much of its value if third parties, such as publishers and producers, were insulated from liability because of their innocence as to the culpability of the persons who supplied them with the infringing material. Furthermore, as between two innocent parties (*i.e.*, the copyright owner and the innocent infringer) it is the latter who should suffer because he, unlike the copyright owner, either has an opportunity to guard against the infringement by diligent inquiry, or at least the ability to guard against liability for infringement by an indemnity agreement from his supplier or by an "errors and omissions" insurance policy.

Nimmer on Copyright, § 13.08, at 13-286.[4]

2. The traditional copyright infringement principles first encountered the Internet in *Playboy Enterprises, Inc. v. Frena*, 839 F. Supp. 1552 (M.D. Fla. 1993).

---

[3] The state of a party's knowledge of the infringing activity may, however, affect the remedies available. *See Fitzgerald*, 807 F.2d at 1113.

[4] Judge Keeton puts the same point in terms of economic principles of risk allocation:

> The enterprise and the person profiting from it are better able than either the innocent injured plaintiff or the person whose act caused the loss to distribute the costs and to shift them to others who have profited from the enterprise. In addition, placing responsibility for the loss on the enterprise has the added benefit of creating a greater incentive for the enterprise to police its operations carefully to avoid unnecessary losses.

Polygram Int'l Publ'g, Inc. v. Nevada/TIG, Inc., 855 F. Supp. 1314, 1325 (D. Mass. 1994).

The defendant in *Frena* operated a subscription "bulletin board service" ("BBS"), to which users could log on, for a fee, and download copies of photographs uploaded by other users. *Id.* at 1554. The plaintiff alleged that it owned the copyright to some of the photographs uploaded onto the BBS. *Id.* The defendant averred that such photographs were uploaded only by subscribers and that as soon as he became aware that plaintiff's copyrighted photographs were available on his BBS, he removed them and continued to monitor the BBS to prevent additional uploads. *Id.*

Under traditional infringement principles, *Frena* was an easy case: the plaintiff's copyrighted photographs were displayed on the defendant's website. Although the defendant contended that he was unaware of what his subscribers were uploading, the court held this to be legally irrelevant: "It does not matter that Defendant Frena may have been unaware of the copyright infringement. Intent to infringe is not needed to find copyright infringement. Intent or knowledge is not an element of infringement, and thus even an innocent infringer is liable for infringement[.]" *Id.* at 1559.

3. While *Frena* was thus a straightforward case under traditional infringement rules, a problem soon became apparent: if traditional infringement rules continued to be applied mechanically in the Internet context, they might quickly engulf the Internet with infringement liability. If those responsible for

copying, distribution and display of material on the Internet were held strictly liable for every infringing "bit" of information they handle, as traditional principles often would dictate, the very existence of the Internet could have been at risk.

The first judicial opinion to recognize and respond to this perceived problem was *Religious Technology Center v. Netcom On-Line Communications Services, Inc.*, 907 F. Supp. 1361 (N.D. Cal. 1995). *Netcom* involved on-line postings about Church of Scientology founder L. Ron Hubbard by former church minister Dennis Erlich. Erlich posted his messages on a "Usenet newsgroup," which he accessed through a BBS operated by Thomas Klemesrud, who in turn linked his BBS to the Internet through Internet service provider Netcom. Contending that Erlich's postings included significant excerpts of copyrighted material, plaintiffs sued not only Erlich, but also Klemesrud and Netcom.

Plaintiffs contended that Netcom and Klemesrud were strictly liable for direct infringement, per *Frena*, because their systems copied Erlich's messages and allowed them to be distributed. The court rejected that claim, but was forced into the "realm of the philosophical," *Nimmer on Copyright* § 12B.01[A][1], at 12B-9, to explain why the potentially devastating risk of liability for Internet service providers rendered plaintiffs' claim simply unacceptable as a matter of policy:

> Plaintiffs' theory would create many separate acts of infringement and, carried to its natural extreme, would lead to unreasonable liability. . . . It would also result in liability for every single Usenet server in the worldwide link of computers transmitting Erlich's

> message to every other computer. These parties, who are liable under plaintiffs' theory, do no more than operate or implement a system that is essential if Usenet messages are to be widely distributed. [907 F. Supp. at 1369-70.]
>
> * * * *
>
> The court does not find workable a theory of infringement that would hold the entire Internet liable for activities that cannot reasonably be deterred. Billions of bits of data flow through the network and are necessarily stored on servers throughout the network and it is practically impossible to screen out infringing bits from noninfringing bits. Because the court cannot see any meaningful distinction (without regard to knowledge) between what Netcom did and what every other Usenet server does, the court finds that Netcom cannot be held liable for direct infringement. [907 F. Supp. at 1372-73.]

For these reasons, the court adopted a special liability-limiting rule for Internet servers: "Although copyright is a strict liability statute, there should still be some element of volition or causation which is lacking when a defendant's system is merely used to create a copy by a third party." *Id.* at 1370. Absent such volition, the court held, an ISP can be sued only for contributory infringement, which requires a plaintiff to prove that the ISP knew or should have known that the postings were infringing. *Id.* at 1369-70. As this Court has recognized, this conclusion effectively erects a categorical bar to traditional, strict liability direct infringement claims against passive ISPs: "[*Netcom*] concluded that when an Internet provider serves, without human intervention, as a passive conduit for copyrighted material, it is not liable as a direct infringer." *ALS Scan, Inc. v. RemarQ Communities, Inc.*, 239 F.3d 619, 622 (4th Cir. 2001).

Netcom's rule of categorical immunity was not a creature of traditional copyright law. To the contrary, as LoopNet itself has correctly observed, it reflected "a dramatic *shift* in copyright law" as applied to ISP defendants, necessitated by the potentially limitless copyright liability they might face without special protections. Doc. 87, at 17 (emphasis added). Rather than applying traditional copyright laws to ISPs as *Frena* had, the *Netcom* court "recognized the inherent *problems* with traditional copyright laws in an Internet context," and therefore "re-evaluated" those laws, *id.* at 2 (emphasis added), to provide special "policy-based protections" for passive ISP defendants, Doc. 107, at 3; *see Nimmer on Copyright* § 12B.01[A][1], at 12B-9 ("At bottom . . . [*Netcom*] reflects a policy judgment as to where the line of liability should be drawn.").

B. *Netcom*'s Special, Policy-Based Protections Were "Codified" In The DMCA

The *Netcom* court may or may not have fairly appraised the policy consequences that might result from a straightforward application of traditional copyright infringement in the Internet context. But such policy considerations are typically the province of the legislative branch, not the judiciary. What is more, *Netcom* was only one district court opinion, and while a few other courts purported to follow its principles, *see, e.g.*, *Marobie-FL, Inc. v. National Ass'n of Fire Equip. Distribs.*, 983 F. Supp. 1167, 1179 (N.D. Ill. 1997); *Sega Enterprises, Ltd. v. MAPHIA*, 948 F. Supp. 923, 932 (N.D. Cal. 1996), other opinions leaned more

toward the traditional rules reflected in *Frena*, *see, e.g.*, *Sega Enterprises, Ltd. v. MAPHIA*, 857 F. Supp. 679, 686 (N.D. Cal. 1994). Rather than leave the law unsettled, exposing copyright owners and ISPs alike to the risks of uneven applications of copyright law to the Internet, Congress resolved the controversy in Title II of the Digital Millennium Copyright Act, 17 U.S.C. § 512. *See* H.R. Rep. No. 105-551(II), at 49 (1998) ("The liability of on-line service providers and Internet access providers for copyright infringements that take place in the online environment has been a controversial issue. Title II of the Digital Millenium Copyright Act addresses this complex issue."); S. Rep. No. 105-190, at 40 (1998).

Congress did not see the problem of copyright infringement only as a problem for ISPs, and it did not enact the DMCA solely to provide ISPs special protections. Rather, Congress understood that the Internet posed novel problems for copyright owners and ISPs alike. On the one hand, the Internet exposed copyright owners to unprecedented risks of endless and instant copying and display of their works, literally worldwide. *See* S. Rep. No. 105-190, at 8 ("Due to the ease with which digital works can be copied and distributed worldwide virtually instantaneously, copyright owners will hesitate to make their works readily available on the Internet without reasonable assurance that they will be protected against massive piracy."). On the other hand, the Internet posed equally unprecedented risks of liability for traditional copyright infringement on ISPs that

handle billions of bits of data, some of which could be infringing. *See id.* ("At the same time, without clarification of their liability, service providers may hesitate to make the necessary investment in the expansion of the speed and capacity of the Internet. In the ordinary course of their operations service providers must engage in all kinds of acts that expose them to potential copyright infringement liability."). The DMCA was written to respond to *both* concerns: "Title II [of the DMCA] preserves strong incentives for service providers and copyright owners to cooperate to detect and deal with copyright infringements that take place in the digital networked environment. At the same time, it provides greater certainty to service providers concerning their legal exposure for infringements that may occur in the course of their activities." *Id.* at 40; H.R. Rep. No. 105-511(II), at 49-50. In this Court's words, the DMCA "was enacted *both* to preserve copyright enforcement on the Internet *and* to provide immunity to service providers from copyright infringement liability for 'passive,' 'automatic' actions in which a service provider's system engages through a technological process initiated by another without the knowledge of the service provider." *ALS Scan*, 239 F.3d at 625 (emphasis added); *see* Paul Goldstein, *Copyright Law* § 6.3, at 6:24 (2d ed. Supp. 2000) (DMCA "carves out several safe harbors that aim to balance the need of copyright owners to obtain effective relief against the need of service providers

to pursue their largely noninfringing activities unencumbered by costly monitoring burdens").

Consistent with its efforts to balance the competing concerns of copyright owners and ISPs, Congress determined that the immunity proposed by the *Netcom* court should *not* be absolute. *ALS Scan*, 239 F.3d at 625. Copyright policy in the Internet era would be best served, Congress concluded, if the immunity envisioned in *Netcom* were available not as a categorical bar to direct infringement claims, but rather as specific "limitations of liability for copyright infringement to which Internet service providers might otherwise be exposed." *Id.* at 623. Accordingly, *Netcom*-type immunity under the DMCA is

> granted only to 'innocent' service providers who can prove they do not have actual or constructive knowledge of the infringement, as defined under any of the three prongs of 17 U.S.C. § 512(c)(1). The DMCA's protection of an innocent service provider disappears at the moment the service provider loses its innocence, i.e., at the moment it becomes aware that a third party is using its system to infringe. At that point, the Act shifts responsibility to the service provider to disable the infringing matter, "preserving the strong incentives for service providers and copyright owners to cooperate to detect and deal with copyright infringements that take place in the digital networked environment."

Id. at 625 (quoting H.R. Conf. Rep. No. 105-796, at 72 (1998)). It is thus the DMCA safe harbor – and only the safe harbor – that reflects "Congress' codification of the *Netcom* principles." *ALS Scan*, 239 F.3d at 622.

In contrast to *Netcom*, the policy balance struck in the DMCA does not altogether prohibit plaintiffs from bringing direct infringement claims against "passive" ISPs. To the contrary, the DMCA presupposes the continued existence of such claims, and responds by codifying the *Netcom* rule as an affirmative defense to such claims. But the affirmative defense is not automatically available to an ISP, even if it is "passive" in *Netcom*'s sense of the word. Rather, any ISP may seek immunity within the DMCA safe harbors – even a non-"passive" ISP – but it must satisfy certain conditions to qualify. Under DMCA § 512(c), an ISP that might otherwise be liable for direct infringement can assert immunity from such a claim "as long as the service provider can show that: (1) it has neither actual knowledge that its system contains infringing materials nor an awareness of facts or circumstances from which an infringement is apparent . . . (2) it receives no financial benefit directly attributable to infringing activity; and (3) it responded expeditiously to remove or disable access to material claimed to be infringing after receiving from the copyright holder a notification conforming with [the] requirements of § 512(c)(3)." *Id.* at 623.[5]

[5] In addition, an ISP must formally designate an agent to receive notification of alleged infringements. 17 U.S.C. § 512(c)(2). An ISP also must have implemented a policy for the identification and termination of users who repeatedly submit infringing material. *Id.* § 512(i)(1)(A). The complete text of § 512, the pertinent section of the DMCA, is reprinted in the Addendum to this brief.

The DMCA safe harbor codifies the immunity proposed by the *Netcom* court, but applies it to all ISPs – not just "passive" ISPs – and reverses the burden of proof. Under *Netcom*, an ISP loses immunity if the plaintiff proves the ISP had knowledge of the infringement (as required by the contributory infringement rubric under which *Netcom* compels plaintiffs to proceed). So, too, under the DMCA, except the ISP must prove that it did *not* have knowledge.[6] But if it cannot meet

[6] DMCA immunity also codifies *Netcom* with respect to the DMCA's "financial benefit" condition. That is, an ISP loses immunity if it fails to prove that it did not obtain a financial benefit directly attributable to the particular activity that is infringing. *Netcom* held the converse: an ISP would be immune unless the plaintiff proved that the ISP obtained a benefit directly tied to the infringing activity itself. 907 F. Supp. at 1377, 1382. According to the legislative history, Congress intended for courts to apply "financial benefit" in accordance with cases "such as *Marobie-FL*," H.R. Rep. No. 105-551(I), at 25 (1998) (emphasis added), which in turn simply followed the *Netcom* court's strict definition of "financial benefit," *see Marobie-FL*, 983 F. Supp. at 1179.

The DMCA "financial benefit" condition does *not*, however, codify the "financial benefit" element of traditional vicarious liability. The financial benefit condition of the DMCA and *Netcom* is much narrower than the traditional "financial benefit" needed to prove vicarious liability. To establish the latter, a plaintiff need only show a general benefit from the infringing activity, i.e., that the activity was part of an overall "draw" for other customers. *See* Goldstein, *Copyright Law* § 6.2.2.1, at 6:22 ("financial benefit will be found where the availability of infringing material in an area under the defendant's control, such as a flea market or Internet site, enhances the present or future value of the defendant's overall operations"); *see, e.g.*, *A&M Records, Inc. v. Napster*, 239 F.3d 1004, 1023 (9th Cir. 2001); *Fonovisa, Inc. v. Cherry Auction, Inc.*, 76 F.3d 259, 264 (9th Cir. 1996); *Polygram Int'l Publ'g, Inc. v. Nevada/TIG, Inc.*, 855 F. Supp. 1314, 1331 (D. Mass. 1994). To establish the financial benefit necessary to strip an ISP of immunity under the DMCA or *Netcom*, by contrast, the financial benefit must be specifically tied to the infringing activity itself, i.e., the defendant gets paid more for infringing activity than non-infringing activity. *See Nimmer on Copyright* § 12B.04[A][3], at 12B-49 ("to the extent that a service provider charges a fee whose value is plainly tied to providing direct access to infringing material, the exemption is lost"); H.R. Rep. No. 105-551(II), at 54 (condition does not apply where "where the infringer makes the same kind of payments as non-infringing users of the provider's service"); S. Rep. No. 105-190, at 44-45. The strict construction of what constitutes a "directly attributable" financial benefit under the DMCA safe harbor "stands in contrast to the gloss on 'direct financial benefit'" applied in evaluating a defendant's underlying vicarious liability in traditional infringement contexts. *Nimmer on Copyright* § 12B.04[A][2], at 12B-48, n.28; *see id.* § 12.04[A][1], at 12-77 & n.27.20 (whereas financial benefit element of vicarious

that burden – or if it otherwise fails to prove its qualification for the safe harbor – then the policy conclusion reflected in the DMCA is that the ISP is *not* an "innocent" ISP deserving of special protection from direct infringement liability. *See ALS Scan*, 239 F.3d at 625; *see also supra* note 6 and *infra* note 7. Accordingly, the plaintiff may proceed with its direct infringement claim against the ISP.

ALS Scan exemplifies the proper treatment of *Netcom*-type defenses to direct infringement claims after the DMCA. *ALS Scan* involved facts similar to both *Netcom* and *Frena*. Plaintiff ALS Scan marketed copyrighted "adult" photographs and other material through a website, CD-ROMs and videotapes. Defendant

---

liability can be established by existence by "possible, indirect benefit," "no such leeway would seem possible" under "financial benefit" condition of DMCA safe harbor).

Because the district court below erroneously believed that the financial benefit element of DMCA/*Netcom* is identical to the traditional financial benefit element for vicarious liability, the court mistakenly suggested that the DMCA provides no immunity for vicarious liability. JA34. Once financial benefit is proved for purposes of establishing vicarious liability, the argument goes, the ISP automatically loses DMCA immunity because it has received the kind of financial benefit that bars it from asserting such immunity. *Id.* But in fact, by *distinguishing* the kind of financial benefit required to establish liability from the kind of financial benefit required to lose immunity, the DMCA both preserves a copyright owner's right to bring a vicarious liability claim and provides a meaningful defense to such a claim for qualified ISPs. *See* H.R. Conf. Rep. No. 105-796, at 73 (DMCA provides immunity from vicarious liability); S. Rep. No. 105-190, at 20 (same); H.R. Rep. No. 105-551(II), at 53 (same). The plaintiff need prove only a general financial benefit to support its prima facie case of vicarious liability, but the ISP will be entitled to immunity if it can show, *inter alia*, that its *particular* financial benefit is *not* of the strictly direct kind contemplated in the DMCA and *Netcom*. If the ISP cannot make that showing, the implicit policy conclusion reflected in the DMCA is that the ISP is not entitled to special protection from vicarious liability, because an ISP that profits so specifically from infringing activity both (a) has a strong incentive to allow infringements, which the law should not protect, and (b) is almost certainly in a good position to monitor and police such activity if the law threatens liability. *See infra* note 7.

RemarQ operated a general service ISP that provided its subscribers access to the Internet, including access to some 30,000 different newsgroups. *Id.* at 620. ALS Scan discovered that several of the newsgroups included many of ALS Scan's copyrighted photographs. ALS Scan notified RemarQ that its website contained the infringing photographs, but RemarQ declined to disable access to them. ALS Scan sued, asserting that RemarQ was liable for both direct infringement and for contributory infringement.

The district court entered summary judgment against plaintiff ALS Scan on its direct infringement claim, relying on the *Netcom* rule. *Id.* at 622. On appeal, ALS Scan urged the court instead to follow the traditional rule applied in *Frena*, *viz.*, that an ISP is strictly liable when it "fail[s] to prevent the placement of plaintiff's copyrighted photographs in its system, despite any proof that the provider had any knowledge of the infringing activities." *Id.* This Court held that although the *Netcom* analysis makes more sense as a matter of policy, it was the DMCA's codification of that policy analysis – not *Netcom* itself – that must control: "Although we find the *Netcom* court reasoning more persuasive, the ultimate conclusion on this point is controlled by Congress' codification of the *Netcom* principles in Title II of the DMCA." *Id.* "Accordingly," the Court concluded, "we address only ALS Scan's claims brought under the DMCA itself." *Id.* The Court then held that RemarQ could not claim the safety of the DMCA's

safe harbor because ALS Scan's notification was adequate under the DMCA. *Id.* at 625-26. The Court therefore reversed summary judgment on the direct infringement claim, and remanded for further proceedings on that claim. *Id.*

ALS Scan thus squarely holds that *Netcom* does *not* preclude direct infringement claims against passive, automatic ISPs, such as RemarQ, that do not qualify for the DMCA safe harbor. To be sure, the Court also observed in a footnote that ALS Scan's claims "would appear" to "amount more to a claim of contributory infringement . . . than to a claim of direct infringement," *id.* at 621 n.1, because ALS Scan alleged that RemarQ had knowledge of the infringement once it was put on notice by ALS Scan. But this footnote did not even suggest, much less hold, that all *other* plaintiffs suing ISPs would be *required* to allege the knowledge inherent to contributory infringement. To the contrary, as noted, the Court even allowed ALS Scan's own claims of direct infringement to go forward.

ALS Scan recognizes that Congress resolved the *Frena*/*Netcom* dichotomy in the DMCA by writing *Netcom*'s protective principles specifically into the text of the safe harbor. Under this structure, it simply makes no sense to say that once an ISP loses the protection of the *Netcom* statutory immunity, it should still benefit from an even more sweeping version of that immunity in the form of an independent, judge-made categorical bar to direct infringement claims. Nothing in the statute or legislative history suggests that Congress intended to provide "double

protection" for ISPs, requiring courts to apply *Netcom*'s principles twice – once through the safe harbor, and then again as independent limitation on a plaintiff's underlying case. Again, just the opposite is true: as noted above, the legislative history repeatedly reports Congress's intention to *balance* the need to "preserve[] strong incentives" to police potential copyright infringements with the need to provide "certainty to [ISPs] concerning their legal exposure for infringements." S. Rep. No. 105-190, at 20, 40; H.R. Rep. No. 105-551[II], at 49-50. Preserving traditional liability rules while providing ISPs a *Netcom*-type defense when they would otherwise be liable under those rules balances the need for certainty with the preservation of strong incentives for lawful behavior; giving an ISP that fails to qualify for DMCA immunity a second dose of immunization under *Netcom* tips that balance in one direction, contrary to Congress's clearly expressed intention.

C. The District Court Erred In Applying *Netcom* As A Categorical Immunity From Direct Infringement Claims Independent Of The DMCA *Netcom*-Type Safe Harbor Immunity

The district court in this case, while quoting at length from *ALS Scan*, actually reached a conclusion directly opposite the one reached in *ALS Scan*. The district court held that the categorical immunity adopted in *Netcom* should *still* apply, even after the DMCA codified that immunity in a more limited form into the text of the DMCA safe harbor. Thus, the district court held, CoStar is categorically barred from pursuing a direct infringement claim against LoopNet – which the

court deemed to be a "passive" ISP under *Netcom* – even though LoopNet does *not* qualify for the safe harbor as to many of the photographs at issue here.

The district court cited nothing in support of that conclusion except *ALS Scan*, but the court simply got that case backwards. The court started by correctly reading *ALS Scan* as having "resolved the dichotomy" between *Netcom* and *Frena*, by recognizing that "Congress had decided the issue, adopting the *Netcom* approach, which [this Court] found more persuasive in any event." JA28. Then the court stated: "As observed by the Fourth Circuit, the *Netcom* approach is more persuasive, *even if not mandated by the DMCA*." *Id.* (emphasis added). And with no further analysis, the court leapt to the conclusion that "this case does not present a valid claim of copyright infringement. . . . Rather, contributory infringement is the proper rubric under which to analyze this case." *Id.*

The district court's error is obvious: this Court in *ALS Scan* did not find *Netcom* "more persuasive" *and therefore applicable of its own force independent of the DMCA.* To the contrary, what the Court held is that although *Netcom* is "more persuasive" than *Frena*, the entire debate is now beside the point, as Congress had decided the issue by codifying the *Netcom* principles *in the terms of the DMCA safe harbor itself.* Nothing in *ALS Scan* or the text or history of the DMCA suggests that Congress intended to "codify" *Netcom* as a super-immunity, over and above what Congress explicitly provided in the statutory safe harbor. In

fact, as noted above, after this Court in *ALS Scan* determined that DMCA immunity was unavailable in that case, it allowed the direct infringement claims to *go forward* – it did not order their dismissal on the basis of *Netcom*. 239 F.3d at 625-26.

Professor David Nimmer nevertheless contends that the text and history of the DMCA does endorse a super-immunity, distinct from what the safe harbor explicitly provides. He argues that even if an ISP fails to qualify for a safe harbor, its conduct "must stand or fall on its own merits, based on how antecedent law would treat it; *Netcom* remains a valuable touchstone in that regard." *Nimmer on Copyright* § 12B.06[B], at 12B-76. Professor Nimmer is half right: it is true that failure to qualify for a safe harbor does not render an ISP "*ipso facto*" liable for infringement, as he puts it, *id.*; a plaintiff must still prove a case of infringement under "antecedent" infringement principles. But it is *not* true that if an ISP fails to qualify for the DMCA safe harbor, the plaintiff's claim still can be categorically barred by *Netcom*'s special judge-made protections for ISPs. *Those* protections exist solely within the terms of the safe harbor.

Professor Nimmer stakes his claim for the continued, independent vitality of *Netcom*'s special rules on two grounds: (1) Congress's expressed intention to "codify" *Netcom*, *see id.* § 12B.06[B], at 12B-76 n.16; *id.* § 12B.05[C]; and (2) the DMCA's statutory assurance that

> [t]he failure of a service provider's conduct to qualify for limitation of liability under this section shall not bear adversely upon the consideration of a defense by the service provider that the service provider's conduct is not infringing under this title or any other defense.

17 U.S.C. § 512(*l*). Neither ground supports his position, or that of the district court in this case.

First, and most clearly, the fact that Congress "codified" *Netcom* in the DMCA does not support the inference that *Netcom* remains a viable touchstone *independent* of the DMCA. The exact opposite is true. Congress "codifies" a principle or rule by *writing it into the statutory code. See Black's Law Dictionary* 252 (7th ed. 1999) ("**codification**: 1. The process of compiling, arranging and systematizing the laws . . . into an ordered code"); *Webster's Third New Int'l Dictionary* 438 (3d ed. rev. 1993) ("codify . . .: 1. to reduce to a code (as laws)"). That is what Congress did here – it wrote the *Netcom* principles *into* the statute, in the form of the safe harbor. Congress does not "codify" the principles of a judicial opinion by leaving them *outside* the code, subject to the vagaries of continued judicial development, restriction, and possible evisceration. If Congress "codified" the *Netcom* principles in the DMCA, as all agree it did, then it can only be *to the DMCA* that we look for enforcement of those principles. And if an ISP falls outside the DMCA's *Netcom* protections – as LoopNet does – then the ISP

necessarily falls outside the scope of the special protection Congress thought it necessary and appropriate to provide.

Second, it follows from all we have shown that § 512(*l*) cannot and does not require a court to give an ISP "double" *Netcom* immunity. On its face, § 512(*l*) is simply a response to the straw-man argument that concerned Professor Nimmer, namely, that "some plaintiff" would argue that the mere failure to qualify for the safe harbor means that the ISP's conduct is "*ipso facto*" barred by copyright law. Such an argument *would* be wrong, and § 512(*l*) removes any doubt on that score. For instance, if an ISP declines to remove material posted on its website upon notification by a plaintiff, or if it receives a financial benefit specifically tied to the allegedly infringing activity, it cannot claim immunity under the safe harbor. But the mere refusal to remove posted material, or the mere fact of the financial benefit, do not, in and themselves, establish that the posted material was, in fact, infringing. That remains a matter for the plaintiff to prove, under antecedent law governing all acts of alleged infringements (not just those of ISPs), as § 512(*l*) simply makes clear.

This system makes perfect sense in terms of the policy balance struck by the DMCA. An ISP can establish its immunity by showing that it is an "innocent" ISP – i.e., that it does not know of or profit directly from allegedly infringing acts. *ALS Scan*, 239 F.3d at 625. Once it is put on proper notice of alleged infringement by a

copyright owner, however, the ISP has a clear opportunity to investigate whether its system is being misused, and to take action if warranted. If the ISP declines to act under those circumstances, there is no *Netcom*-type policy reason why it *should* get extra protection from copyright liability under traditional rules.[7] If such an ISP takes itself outside the DMCA safe harbor by declining to act, then it should be subject to the same risk of copyright liability as any other defendant, under the same traditional copyright rules that would apply to any other defendant.

D. Absent *Netcom* Immunity, LoopNet Was Not Entitled To Summary Judgment On Its Direct Infringement Claims

The district court summarily dismissed CoStar's direct infringement claim without any analysis other than an erroneous reading of *ALS Scan*, which led to an improper application of a categorical *Netcom* immunity. Thus the court did not even reach the DMCA safe harbor before dismissing the direct infringement claim. The court nevertheless did analyze LoopNet's status under the safe harbor, because LoopNet asserted it as a defense to CoStar's separate claim of contributory infringement – the one claim the court said could proceed under *Netcom*.

The district court held that LoopNet was *not* entitled to summary judgment on its claim of immunity under the safe harbor. Specifically, LoopNet failed to

[7] The same is true for an ISP that loses its immunity because it receives a financial benefit that is specifically tied to infringing activity. Under those circumstances, the ISP will certainly have reason, and likely the ability, to monitor and control the conduct, and thus deserves no special immunity from application of traditional copyright rules. *See supra* note 6.

prove its qualification for the safe harbor in two respects. First, LoopNet had not designated the DMCA-required agent to receive notifications of claimed infringements until December 8, 1999 – after CoStar filed this action. JA29 n.4. "Therefore," the court held, "the safe harbor is only available to LoopNet with regard to its liability (if any) arising after that date." *Id.* Second, the court concluded that "several material factual disputes remain[ed]" as to whether LoopNet had satisfied the safe harbor requirements that an ISP "expeditiously" remove or block access to claimed infringing material upon proper notification by a copyright owner, and that an ISP adopt a policy for dealing with repeat infringers. JA33. In short, the court concluded that LoopNet had failed to prove its entitlement to the safe harbor for the set of claims relating to photographs (a) displayed prior to December 8, 1999, and (b) that LoopNet did not expeditiously take down or have a policy for handling.

As to the pre-December 8, 1999 direct infringement claims, the district court should have entered summary judgment in CoStar's favor. LoopNet concedes that it was not entitled to DMCA immunity for those claims, and we have shown why *Netcom* immunity can no longer prevail. Absent such immunities, CoStar's case for direct infringement on the undisputed record facts is irrefutable. CoStar owns the photographs, and LoopNet copied, distributed and displayed them on its website. Nothing more is needed to prove a traditional direct infringement claim.

See supra at 16-17 (describing two elements of direct infringement: ownership and copying/distribution/display). "With respect to the allowance of uploading material by their subscribers, [ISPs] act essentially as an electronic publisher," Information Infrastructure Task Force, *Intellectual Property and the National Information Infrastructure: Report of the Working Group on Intellectual Property Rights* 122 (1995), and therefore are, under traditional copyright principles, strictly liable for infringing conduct just like any other publisher – even an unwitting publisher – of infringing material, *see id.* at 116 (observing that "photo finishers . . . book sellers, record stores, newsstands and computer software retailers . . . may be held strictly liable as distributors if the works or copies they deal in are infringing"); *see, e.g.*, *Playboy Enterprises, Inc. v. Frena*, 839 F. Supp. 1552 (M.D. Fla. 1993) (computer BBS strictly liable for infringing postings of users); *Playboy Enterprises, Inc. v. Russ Hardenburgh, Inc.*, 982 F. Supp. 503 (N.D. Ohio 1997) (computer BBS strictly liable for infringing postings of users); *see generally* Jane C. Ginsburg, *Putting Cars On the "Information Superhighway": Authors, Exploiters, and Copyright In Cyberspace*, 95 Colum. L. Rev. 1466, 1494 (1995) (discussing application of traditional, pre-*Netcom* copyright principles to ISPs: "As a result of the technology of communication on digital networks (at least for now), the online service [provider] is itself engaging in acts of copyright exploitation. When a user posts a work on the bulletin board, a 'copy' of the work

is made in the service's server. When the work is communicated to subscribers, it is 'publicly performed or displayed' on their screens."); Paul Goldstein, *Copyright, Patent, Trademark and Related State Doctrines* 732 (2002) (suggesting comparison of ISPs to "book or record store owners who are subject to strict liability for public distribution of infringing copies or phonorecords" and to "photo finishers who process millions of copyrighted photographs each day and are also strictly liable").

As to the post-December 8, 1999 claims, LoopNet is entitled at least to *assert* DMCA immunity. But as the district court held, continued factfinding is necessary to establish whether LoopNet properly disabled access to certain photographs, and whether LoopNet had an adequate policy for terminating repeat infringers. If LoopNet can make those showings, LoopNet is entitled to summary judgment; if not, CoStar is entitled to summary judgment.

In short, this Court should reverse the district court's summary judgment order, remand the pre-December 8, 1999 claims with instructions to enter judgment for CoStar, and remand the remainder for further factfinding as to LoopNet's satisfaction of the DMCA's requirements. Alternatively, the Court could simply correct the fundamental error of law underlying the summary judgment order and remand all the direct infringement claims for further analysis under the proper copyright standards, without the special policy influences of *Netcom* now cabined

within the DMCA's statutory immunity. Given that not even *the district court* has ever addressed the basic summary judgment question in respect to direct infringement, this Court may wish to vacate and remand the case for the district court to do so in the first instance. What matters most for purposes of this appeal is that this Court correct the district court's misunderstanding of the role of *Netcom* immunity in post-DMCA copyright law.

II. LOOPNET DOES NOT QUALIFY FOR *NETCOM* IMMUNITY EVEN UNDER *NETCOM*'S OWN TERMS BECAUSE LOOPNET IS NOT A "PASSIVE" ISP

Even assuming that, contrary to *ALS Scan*, the district court correctly perceived that *Netcom* immunity *could* apply to an ISP that does not qualify for DMCA immunity, the district court was nevertheless wrong to conclude that *Netcom* immunity *does* apply to LoopNet.

Netcom immunity applies only to "passive" ISPs, through which data flow is "automatic." This Court itself described the *Netcom* rule as: "[W]hen an Internet provider serves, *without human intervention*, as a *passive conduit* for copyrighted material, it is not liable as a direct infringer." *ALS Scan*, 239 F.3d at 622 (emphasis added). The *Netcom* rule was devised to protect from copyright liability computer systems that blindly transmit data bits with no realistic way for the system operator to monitor their content. The *Netcom* court's concern, its opinion

makes clear, was with imposing liability *only* for those for activities that are *essential* for the basic functioning of the entire Internet:

> [P]laintiffs' theory further implicates a Usenet server that carries Erlich's message to other servers regardless of whether that server acts without any human intervention beyond the initial setting up of the system. It would also result in liability for every single Usenet server in the worldwide link of computers transmitting Erlich's message to every other computer. These parties, who are liable under plaintiffs' theory, do *no more than* operate or implement a system that is essential if Usenet messages are to be widely distributed. There is no need to construe the Act to make all of these parties infringers. Although copyright is a strict liability statute, there should still be some element of volition or causation which is lacking where a defendant's system is *merely* used to create a copy by a third party.

907 F. Supp. at 1369-70 (emphasis added). Thus by its own terms the *Netcom* rule was *not* intended to protect ISPs that do anything "more than" what is minimally necessary to facilitate the functioning of the Internet. The *Netcom* court makes the point repeatedly. *See also id.* at 1368 ("Netcom did not take any affirmative action that directly resulted in copying plaintiffs' works *other than* by installing and maintaining a system whereby software automatically forwards messages received from subscribers onto the Usenet, and temporarily stores copies on its system" (emphasis added)); *id.* at 1372 ("it does not make sense to adopt a rule that could lead to the liability of countless parties whose role in the infringement is *nothing more than* setting up and operating a system that is necessary for the functioning of the Internet" (emphasis added)). And the court emphasized, in particular, that Netcom's technological activities had nothing whatsoever to do

with control of content: "In contrast to some of its larger competitors, Netcom does not create or control the content of the information available to its subscribers; it merely provides *access* to the Internet, whose content is controlled by no single entity." *Id.* at 1368.

It is plain to see that the *Netcom* court was *not* concerned with the type of situation involved here. Unlike Netcom, LoopNet *does* control the content of material posted on its website: only commercial real estate information is allowed, and nothing else. *See supra* at 11-12. LoopNet employs human reviewers not just as gatekeepers to screen out obscenity or pornography and the like – technological tools can do that – but to ensure that the content does not deviate from LoopNet's commercially-based prescription. *Id.* LoopNet does not "merely provide access" to the Internet; what it provides is the opportunity to post specific types of material, the content of which is specifically intended to attract other users, who would then view the advertising LoopNet sold on its site. All of those activities – creating a content-based commercial website, screening material posted for consistency with its content prescriptions, selling advertising based on the draw of the content to other users – are "volitional" activities that specifically encourage and channel the conduct that results in infringement. LoopNet obviously has done much more than "set[] up and operat[e] a system that is necessary for the functioning of the Internet." *Id.* at 1372. Holding LoopNet liable for material posted on its subject-

matter-controlled, commercial website would in no way risk liability for the truly passive, automatic purveyors of electronic information that are essential to the operation of the Internet.

This case cannot be distinguished from *Playboy Enterprises, Inc. v. Russ Hardenburgh, Inc.*, 982 F. Supp. 503 (N.D. Ohio 1997), a post-*Netcom*, pre-DMCA case that applied *Netcom*'s "volition" element to deny immunity under the same set of material facts. The defendant in that case operated a BBS to which users posted materials, including adult photographs. Playboy sued alleging that many of the photographs were owned by Playboy. The BBS operator sought immunity from direct infringement under *Netcom*, but the court found that the BBS was not a "passive" provider because of "two crucial facts": (1) the BBS operator had a "policy of encouraging subscribers to upload files, including adult photographs, onto the system," and (2) the BBS operator employed "a screening procedure in which [the operator's] employees *viewed* all files in the upload file and *moved them* into the generally available files for subscribers." *Id.* at 513. "The two facts," the court held, "transform Defendants from passive providers of a space in which infringing activities happened to occur to active participants in the process of copyright infringement." *Id.*

Exactly the same "two crucial facts" are present here. LoopNet encourages users to post real estate information, including photographs, on its website.

Indeed, that is LoopNet's commercial *raison d'être*. LoopNet employees view all the postings and, if deemed appropriate, move them onto LoopNet's website. Those activities transform LoopNet from a passive ISP where infringements may just happen to occur, to an active participant, no different than a seller of infringing real estate books. Accordingly, LoopNet, like the defendant in *Russ Hardenburgh*, is not entitled to the special immunity *Netcom* reserved for truly passive, automatic ISPs. *See also Playboy Enterprises, Inc. v. Webbworld, Inc.*, 991 F. Supp. 543, 552 (N.D. Tex. 1997) (refusing to apply *Netcom* immunity to defendant that "did not function as a mere provider of access," but instead provided particular content and functioned as a "commercial destination within the Internet").

The district court's conclusion to the contrary is insupportable. The court made no effort to address the fact that LoopNet explicitly encourages users to post material, one of the facts the *Russ Hardenburgh* court found "crucial" to its conclusion that the ISP in that case was not "passive" like Netcom. Indeed, the district court did not address *Russ Hardenburgh*'s analysis or holding on this point at all, even though it was amply discussed in CoStar's briefs.

The court instead held that LoopNet is a "passive" ISP within the meaning of *Netcom* simply because the uploading of photographs is "initiated" by LoopNet's users. JA27. Later in its opinion, in the course of discussing an entirely separate issue, the court elaborated the point slightly. CoStar argued

below that photographs on LoopNet's website are not "stored at the direction of a user" – and thus the DMCA § 512(c) safe harbor is inapplicable – because it is LoopNet, not the user, that has final say in selecting and uploading photographs. In response that argument, the court stated: "[The photographs] are uploaded at the volition of the user and are subject, not to a review and selection process, but to a mere screening to assess whether they are commercial property and to catch any obvious infringements. Although humans are involved rather than mere technology, they serve only as a gateway and are not involved in a selection process." JA32; *see also* JA31 n.6 ("whether the uploading process is controlled by technological or human barriers is irrelevant"). Thus the district court's holding appears to be that *Netcom* immunity applies whenever a user "initiates" the process of uploading material – i.e., a message or photograph – even if, as here, the ISP employs a system of human screening for every submission to ensure that its content is within the narrow range prescribed by the ISP in order to further its commercial goals. This is quite wrong.

To start, the court's dismissal of the relevance of LoopNet's process of *human* screening flies directly in the face of both *Netcom* and *ALS Scan*, both of which explicitly identified the lack of "*human* intervention" with respect to the posting and messaging processes as the key factor that rendered Netcom a "passive" ISP entitled to special protection from copyright liability. *ALS Scan*, 239

F.3d at 622; *see Netcom*, 907 F. Supp. at 1369. Nor was this just a linguistic fancy. As discussed above, the whole point of *Netcom* was that the entire Internet might be overrun with copyright liability if ISPs that "do *no more than* operate or implement a system that is essential" to the functioning of the Internet can be held liable for the infringing bits that flow through their systems. 907 F. Supp. at 1369-70 (emphasis added)); *see id.* at 1372 (rejecting liability for ISPs that do "*nothing more than* set[] up and operat[e] a system that is necessary for the functioning of the Internet" (emphasis added). Netcom was held to be immune because it "*merely* provides *access* to the Internet." *Id.* at 1372 (first emphasis added). The fact that an ISP's system operates with significant human involvement – i.e., individual screening of every single photograph posted – is a near-certain indicator that the system is doing something *more* than just providing access and operating the basic technology essential to the functioning of the Internet.

Thus the fact that LoopNet employs a system of human screening is enough in and of itself to establish that LoopNet is not a "passive" ISP within the meaning of *Netcom*. But here there is still more. The "volition" LoopNet exercises is not reflected solely in its human screening. It includes the additional facts that LoopNet encourages users to post material; that LoopNet actively and strictly limits the content of *all* postings to the prescribed set of real estate information so that other users will be attracted to the website; and that LoopNet not only screens

but sometimes edits photographs to keep them consistent with a certain quality commercial message that LoopNet "sells" to other potential users. All of those facts make this case much more like *Russ Hardenburgh* – and nothing whatsoever like *Netcom*. In short, exercising "volition" means more than just initiating uploads; it means actively controlling, through human intervention if necessary, the content of the information conveyed or displayed by the ISP. That is precisely what LoopNet does, which is precisely why it is not a "passive" ISP.

* * * *

Except for the electronic medium in which it operates, an ISP that copies, distributes, or displays infringing material is just like any another copier, distributor, or displayer of infringing material. To the extent the electronic medium makes a difference, Congress has prescribed just what kind of difference it should make. An ISP that does not qualify for the special protection Congress has chosen to provide should not receive any additional protection. It should be treated by the law just like any other entity that has conveyed or displayed infringing material. If LoopNet received CoStar's photographs from users in paper form and passed them around to other users, or sold them in a bookstore, or posted them on a wall outside its headquarters, LoopNet would be liable for direct infringement. Instead LoopNet posts them electronically on its website. Because of that one distinguishing fact, Congress would have allowed LoopNet to escape the liability

that would otherwise have been strictly imposed, except that LoopNet has failed to satisfy the conditions Congress prescribed for receiving such special treatment. The district court's decision nevertheless to afford LoopNet special immunity from copyright liability for conduct that would be infringing in any other medium is incorrect and should be reversed.

CONCLUSION

For the foregoing reasons, the district court's order of summary judgment for LoopNet on CoStar's claims for direct copyright infringement should be reversed. The case should be remanded for entry of judgment for CoStar for all direct infringement claims involving photographs posted prior to December 8, 1999, and for further factfinding with respect to all other direct infringement claims.

Respectfully submitted,

WALTER DELLINGER
JONATHAN D. HACKER
O'MELVENY & MYERS LLP
1625 Eye Street, N.W.
Washington, D.C. 20006
(202) 383-5300

Counsel for Appellants

CERTIFICATE OF COMPLIANCE

I hereby certify that the foregoing Brief of Appellant complies with the type-volume limitations prescribed by Fed. R. App. P. 32(a)(7)(B)(i). The brief contains 11,693 words.

_____
Jonathan D. Hacker

CERTIFICATE OF SERVICE

I hereby certify that on October 15, 2003, I caused two copies of the foregoing Brief of Appellant to be served by first-class mail, postage pre-paid, on the following counsel:

Kenneth Wilson
Kurt B. Opsahl
Perkins Coie LLP
180 Townsend Street
San Francisco, CA 94107

_____
Jonathan D. Hacker

ADDENDUM

Digital Millennium Copyright Act Safe Harbors, 17 U.S. § 512

Section 512. Limitations on liability relating to material online

(a) Transitory Digital Network Communications. - 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 provider'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, if -

(1) the transmission of the material was initiated by or at the direction of a person other than the service provider;

(2) the transmission, routing, provision of connections, or storage is carried out through an automatic technical process without selection of the material by the service provider;

(3) the service provider does not select the recipients of the material except as an automatic response to the request of another person;

(4) no copy of the material made by the service provider in the course of such intermediate or transient storage is maintained on the system or network in a manner ordinarily accessible to anyone other than anticipated recipients, and no such copy is maintained on the system or network in a manner ordinarily accessible to such anticipated recipients for a longer period than is reasonably necessary for the transmission, routing, or provision of connections; and

(5) the material is transmitted through the system or network without modification of its content.

(b) System Caching. -

(1) Limitation on liability. - 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 intermediate and temporary storage of material on a system or network controlled or operated by or

for the service provider in a case in which -

(A) the material is made available online by a person other than the service provider;

(B) the material is transmitted from the person described in subparagraph (A) through the system or network to a person other than the person described in subparagraph (A) at the direction of that other person; and

(C) the storage is carried out through an automatic technical process for the purpose of making the material available to users of the system or network who, after the material is transmitted as described in subparagraph (B), request access to the material from the person described in subparagraph (A),

if the conditions set forth in paragraph (2) are met.

(2) Conditions. - The conditions referred to in paragraph (1) are that -

(A) the material described in paragraph (1) is transmitted to the subsequent users described in paragraph (1)(C) without modification to its content from the manner in which the material was transmitted from the person described in paragraph (1)(A);

(B) the service provider described in paragraph (1) complies with rules concerning the refreshing, reloading, or other updating of the material when specified by the person making the material available online in accordance with a generally accepted industry standard data communications protocol for the system or network through which that person makes the material available, except that this subparagraph applies only if those rules are not used by the person described in paragraph (1)(A) to prevent or unreasonably impair the intermediate storage to which this subsection applies;

(C) the service provider does not interfere with the ability of technology associated with the material to return to the person described in paragraph (1)(A) the information that would have been available to that person if the material had been obtained by the subsequent users described in paragraph (1)(C) directly from that person, except that this subparagraph applies only if that technology -

(i) does not significantly interfere with the performance of the provider's system or network or with the intermediate storage of the material;

(ii) is consistent with generally accepted industry standard communications protocols; and

(iii) does not extract information from the provider's system or network other than the information that would have been available to the person described in paragraph (1)(A) if the subsequent users had gained access to the material directly from that person;

(D) if the person described in paragraph (1)(A) has in effect a condition that a person must meet prior to having access to the material, such as a condition based on payment of a fee or provision of a password or other information, the service provider permits access to the stored material in significant part only to users of its system or network that have met those conditions and only in accordance with those conditions; and

(E) if the person described in paragraph (1)(A) makes that material available online without the authorization of the copyright owner of the material, the service provider responds expeditiously to remove, or disable access to, the material that is claimed to be infringing upon notification of claimed infringement as described in subsection (c)(3), except that this subparagraph applies only if -

(i) the material has previously been removed from the originating site or access to it has been disabled, or a court has ordered that the material be removed from the originating site or that access to the material on the originating site be disabled; and

(ii) the party giving the notification includes in the notification a statement confirming that the material has been removed from the originating site or access to it has been disabled or that a court has ordered that the material be removed from the originating site or that access to the material on the originating site be disabled.

(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;

(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.

(2) Designated agent. - The limitations on liability established in this subsection apply to a service provider only if the service provider has designated an agent to receive notifications of claimed infringement described in paragraph (3), by making available through its service, including on its website in a location accessible to the public, and by providing to the Copyright Office, substantially the following information:

(A) the name, address, phone number, and electronic mail address of the agent.

(B) other contact information which the Register of Copyrights may deem appropriate.

The Register of Copyrights shall maintain a current directory of agents available to the public for inspection, including through the Internet, in both electronic and hard copy formats, and may require payment of a fee by service providers to cover the costs of maintaining the directory.

(3) Elements of notification. -

(A) To be effective under this subsection, a notification of claimed infringement must be a written communication provided to the designated agent of a service provider that includes substantially the following:

(i) A physical or electronic signature of a person

authorized to act on behalf of the owner of an exclusive right that is allegedly infringed.

(ii) Identification of the copyrighted work claimed to have been infringed, or, if multiple copyrighted works at a single online site are covered by a single notification, a representative list of such works at that site.

(iii) Identification of the material that is claimed to be infringing or to be the subject of infringing activity and that is to be removed or access to which is to be disabled, and information reasonably sufficient to permit the service provider to locate the material.

(iv) Information reasonably sufficient to permit the service provider to contact the complaining party, such as an address, telephone number, and, if available, an electronic mail address at which the complaining party may be contacted.

(v) A statement that the complaining party has a good faith belief that use of the material in the manner complained of is not authorized by the copyright owner, its agent, or the law.

(vi) A statement that the information in the notification is accurate, and under penalty of perjury, that the complaining party is authorized to act on behalf of the owner of an exclusive right that is allegedly infringed.

(B)(i) Subject to clause (ii), a notification from a copyright owner or from a person authorized to act on behalf of the copyright owner that fails to comply substantially with the provisions of subparagraph (A) shall not be considered under paragraph (1)(A) in determining whether a service provider has actual knowledge or is aware of facts or circumstances from which infringing activity is apparent.

(ii) In a case in which the notification that is provided to the service provider's designated agent fails to comply substantially with all the provisions of subparagraph (A) but substantially complies with clauses (ii), (iii), and (iv) of subparagraph (A), clause (i) of this subparagraph applies only if the service provider promptly attempts to contact the person making the notification or takes other reasonable steps to assist in the receipt of notification that substantially complies with all the provisions of subparagraph (A).

(d) Information Location Tools. - 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 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, if the service provider -

(1)(A) does not have actual knowledge that the material or activity is infringing;

(B) in the absence of such actual knowledge, is not aware of facts or circumstances from which infringing activity is apparent; or

(C) upon obtaining such knowledge or awareness, acts expeditiously to remove, or disable access to, the material;

(2) 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

(3) upon notification of claimed infringement as described in subsection (c)(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, except that, for purposes of this paragraph, the information described in subsection (c)(3)(A)(iii) shall be identification of the reference or link, to material or activity claimed to be infringing, that is to be removed or access to which is to be disabled, and information reasonably sufficient to permit the service provider to locate that reference or link.

(e) Limitation on Liability of Nonprofit Educational Institutions. - (1) When a public or other nonprofit institution of higher education is a service provider, and when a faculty member or graduate student who is an employee of such institution is performing a teaching or research function, for the purposes of subsections (a) and (b) such faculty member or graduate student shall be considered to be a person other than the institution, and for the purposes of subsections (c) and (d) such faculty member's or graduate student's knowledge or awareness of his or her infringing activities shall not be attributed to the institution, if -

(A) such faculty member's or graduate student's infringing activities do not involve the provision of online access to instructional materials that are or were required or recommended, within the preceding 3-year period, for a course taught at the institution by such faculty member or graduate student;

(B) the institution has not, within the preceding 3-year period, received more than two notifications described in subsection (c)(3) of claimed infringement by such faculty member or graduate student, and such notifications of claimed infringement were not actionable under subsection (f); and

(C) the institution provides to all users of its system or network informational materials that accurately describe, and promote compliance with, the laws of the United States relating to copyright.

(2) For the purposes of this subsection, the limitations on injunctive relief contained in subsections (j)(2) and (j)(3), but not those in (j)(1), shall apply.

(f) Misrepresentations. - Any person who knowingly materially misrepresents under this section -

(1) that material or activity is infringing, or

(2) that material or activity was removed or disabled by mistake or misidentification,

shall be liable for any damages, including costs and attorneys' fees, incurred by the alleged infringer, by any copyright owner or copyright owner's authorized licensee, or by a service provider, who is injured by such misrepresentation, as the result of the service provider relying upon such misrepresentation in removing or disabling access to the material or activity claimed to be infringing, or in replacing the removed material or ceasing to disable access to it.

(g) Replacement of Removed or Disabled Material and Limitation on Other Liability. -

(1) No liability for taking down generally. - Subject to paragraph (2), a service provider shall not be liable to any person for any claim based on the service provider's good faith disabling of access to, or removal of, material or activity claimed to be infringing or based on facts or circumstances from which infringing activity is apparent, regardless of whether the

material or activity is ultimately determined to be infringing.

(2) Exception. - Paragraph (1) shall not apply with respect to material residing at the direction of a subscriber of the service provider on a system or network controlled or operated by or for the service provider that is removed, or to which access is disabled by the service provider, pursuant to a notice provided under subsection (c)(1)(C), unless the service provider -

(A) takes reasonable steps promptly to notify the subscriber that it has removed or disabled access to the material;

(B) upon receipt of a counter notification described in paragraph (3), promptly provides the person who provided the notification under subsection (c)(1)(C) with a copy of the counter notification, and informs that person that it will replace the removed material or cease disabling access to it in 10 business days; and

(C) replaces the removed material and ceases disabling access to it not less than 10, nor more than 14, business days following receipt of the counter notice, unless its designated agent first receives notice from the person who submitted the notification under subsection (c)(1)(C) that such person has filed an action seeking a court order to restrain the subscriber from engaging in infringing activity relating to the material on the service provider's system or network.

(3) Contents of counter notification. - To be effective under this subsection, a counter notification must be a written communication provided to the service provider's designated agent that includes substantially the following:

(A) A physical or electronic signature of the subscriber.

(B) Identification of the material that has been removed or to which access has been disabled and the location at which the material appeared before it was removed or access to it was disabled.

(C) A statement under penalty of perjury that the subscriber has a good faith belief that the material was removed or disabled as a result of mistake or misidentification of the material to be removed or disabled.

(D) The subscriber's name, address, and telephone number, and a statement that the subscriber consents to the jurisdiction of Federal District Court for the judicial district in which the address is located, or if the subscriber's address is outside

of the United States, for any judicial district in which the service provider may be found, and that the subscriber will accept service of process from the person who provided notification under subsection (c)(1)(C) or an agent of such person.

(4) Limitation on other liability. - A service provider's compliance with paragraph (2) shall not subject the service provider to liability for copyright infringement with respect to the material identified in the notice provided under subsection (c)(1)(C).

(h) Subpoena To Identify Infringer. -

(1) Request. - A copyright owner or a person authorized to act on the owner's behalf may request the clerk of any United States district court to issue a subpoena to a service provider for identification of an alleged infringer in accordance with this subsection.

(2) Contents of request. - The request may be made by filing with the clerk -

(A) a copy of a notification described in subsection (c)(3)(A);

(B) a proposed subpoena; and

(C) a sworn declaration to the effect that the purpose for which the subpoena is sought is to obtain the identity of an alleged infringer and that such information will only be used for the purpose of protecting rights under this title.

(3) Contents of subpoena. - The subpoena shall authorize and order the service provider receiving the notification and the subpoena to expeditiously disclose to the copyright owner or person authorized by the copyright owner information sufficient to identify the alleged infringer of the material described in the notification to the extent such information is available to the service provider.

(4) Basis for granting subpoena. - If the notification filed satisfies the provisions of subsection (c)(3)(A), the proposed subpoena is in proper form, and the accompanying declaration is properly executed, the clerk shall expeditiously issue and sign the proposed subpoena and return it to the requester for delivery to the service provider.

(5) Actions of service provider receiving subpoena. - Upon

receipt of the issued subpoena, either accompanying or subsequent to the receipt of a notification described in subsection (c)(3)(A), the service provider shall expeditiously disclose to the copyright owner or person authorized by the copyright owner the information required by the subpoena, notwithstanding any other provision of law and regardless of whether the service provider responds to the notification.

(6) Rules applicable to subpoena. - Unless otherwise provided by this section or by applicable rules of the court, the procedure for issuance and delivery of the subpoena, and the remedies for noncompliance with the subpoena, shall be governed to the greatest extent practicable by those provisions of the Federal Rules of Civil Procedure governing the issuance, service, and enforcement of a subpoena duces tecum.

(i) Conditions for Eligibility. -

(1) Accommodation of technology. - The limitations on liability established by this section shall apply to a service provider only if the service provider -

(A) has adopted and reasonably implemented, and informs subscribers and account holders of the service provider's system or network of, a policy that provides for the termination in appropriate circumstances of subscribers and account holders of the service provider's system or network who are repeat infringers; and

(B) accommodates and does not interfere with standard technical measures.

(2) Definition. - As used in this subsection, the term "standard technical measures" means technical measures that are used by copyright owners to identify or protect copyrighted works and -

(A) have been developed pursuant to a broad consensus of copyright owners and service providers in an open, fair, voluntary, multi-industry standards process;

(B) are available to any person on reasonable and nondiscriminatory terms; and

(C) do not impose substantial costs on service providers or substantial burdens on their systems or networks.

(j) Injunctions. - The following rules shall apply in the case of

any application for an injunction under section 502 against a service provider that is not subject to monetary remedies under this section:

(1) Scope of relief. - (A) With respect to conduct other than that which qualifies for the limitation on remedies set forth in subsection (a), the court may grant injunctive relief with respect to a service provider only in one or more of the following forms:

(i) An order restraining the service provider from providing access to infringing material or activity residing at a particular online site on the provider's system or network.

(ii) An order restraining the service provider from providing access to a subscriber or account holder of the service provider's system or network who is engaging in infringing activity and is identified in the order, by terminating the accounts of the subscriber or account holder that are specified in the order.

(iii) Such other injunctive relief as the court may consider necessary to prevent or restrain infringement of copyrighted material specified in the order of the court at a particular online location, if such relief is the least burdensome to the service provider among the forms of relief comparably effective for that purpose.

(B) If the service provider qualifies for the limitation on remedies described in subsection (a), the court may only grant injunctive relief in one or both of the following forms:

(i) An order restraining the service provider from providing access to a subscriber or account holder of the service provider's system or network who is using the provider's service to engage in infringing activity and is identified in the order, by terminating the accounts of the subscriber or account holder that are specified in the order.

(ii) An order restraining the service provider from providing access, by taking reasonable steps specified in the order to block access, to a specific, identified, online location outside the United States.

(2) Considerations. - The court, in considering the relevant criteria for injunctive relief under applicable law, shall consider -

(A) whether such an injunction, either alone or in

combination with other such injunctions issued against the same service provider under this subsection, would significantly burden either the provider or the operation of the provider's system or network;

(B) the magnitude of the harm likely to be suffered by the copyright owner in the digital network environment if steps are not taken to prevent or restrain the infringement;

(C) whether implementation of such an injunction would be technically feasible and effective, and would not interfere with access to noninfringing material at other online locations; and

(D) whether other less burdensome and comparably effective means of preventing or restraining access to the infringing material are available.

(3) Notice and ex parte orders. - Injunctive relief under this subsection shall be available only after notice to the service provider and an opportunity for the service provider to appear are provided, except for orders ensuring the preservation of evidence or other orders having no material adverse effect on the operation of the service provider's communications network.

(k) Definitions. -

(1) Service provider. - (A) As used in subsection (a), the term "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.

(B) As used in this section, other than subsection (a), the term "service provider" means a provider of online services or network access, or the operator of facilities therefor, and includes an entity described in subparagraph (A).

(2) Monetary relief. - As used in this section, the term "monetary relief" means damages, costs, attorneys' fees, and any other form of monetary payment.

(*l*) Other Defenses Not Affected. - The failure of a service provider's conduct to qualify for limitation of liability under this section shall not bear adversely upon the consideration of a defense by the service provider that the service provider's conduct

is not infringing under this title or any other defense.

(m) Protection of Privacy. - Nothing in this section shall be construed to condition the applicability of subsections (a) through (d) on -

(1) a service provider monitoring its service or affirmatively seeking facts indicating infringing activity, except to the extent consistent with a standard technical measure complying with the provisions of subsection (i); or

(2) a service provider gaining access to, removing, or disabling access to material in cases in which such conduct is prohibited by law.

(n) Construction. - Subsections (a), (b), (c), and (d) describe separate and distinct functions for purposes of applying this section. Whether a service provider qualifies for the limitation on liability in any one of those subsections shall be based solely on the criteria in that subsection, and shall not affect a determination of whether that service provider qualifies for the limitations on liability under any other such subsection.