

1 Cindy A. Cohn (SBN 145997)
cindy@eff.org
2 Jason M. Schultz (SBN 212600)
jason@eff.org
3 Corynne McSherry (SBN 221504)
corynne@eff.org
4 ELECTRONIC FRONTIER FOUNDATION
454 Shotwell Street
5 San Francisco, CA 94110
Telephone: (415) 436-9333
6 Facsimile: (415) 436-9993
7 Attorneys for Amicus Curiae
ELECTRONIC FRONTIER FOUNDATION
8
9

10 UNITED STATES DISTRICT COURT
11 FOR THE NORTHERN DISTRICT OF CALIFORNIA
12 SAN FRANCISCO DIVISION

13 *In re:*)
14 LOOPNET, INC.)
Subpoena Enforcement Matter) MISCELLANEOUS ACTION
15) Case No. CV 05-80294 – Misc. VRW (JL)
16 COSTAR REALTY, INC., a Delaware)
corporation and COSTAR REALTY) **AMICUS CURIAE BRIEF OF**
17 INFORMATION, INC., a Delaware corporation) **ELECTRONIC FRONTIER**
) **FOUNDATION IN SUPPORT OF**
18 v.) **LOOPNET, INC.**
)
19 LOOPNET, INC, a California corporation.) Date: Aug 2, 2006
) Time: 9:00 a.m.
20) Courtroom: F (15th Floor)
) Judge: The Hon. James Larson
21 _____)

TABLE OF CONTENTS

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

- I. INTRODUCTION AND SUMMARY OF ARGUMENT 1
- II. INTERESTS OF AMICUS 3
- III. BACKGROUND 3
- IV. ARGUMENT 6
 - A. The Court Must Balance CoStar’s Litigation Interests Against the Anonymous Downloaders’ Free Speech Interests. 6
 - 1. Efforts To Use The Power Of The Courts To Pierce Anonymity Are Subject To A Qualified Privilege. 6
 - a. The First Amendment protects anonymous online communication. 6
 - b. Anonymous online communication is subject to a qualified privilege. 7
 - 2. The Qualified Privilege Requires the Evaluation Of Multiple Factors Prior to Subpoena Enforcement 8
 - B. The Complexities of Copyright Law and the Potential for Misuse of Section 512(h) Requires Application of A “Sony Entertainment Plus” Standard 11
 - 1. The Complexities of Copyright Law and the Potential for Misuse of Section 512(h) raise serious concerns under the First Amendment 11
 - 2. The “Sony Plus” test properly balances 512(h) subpoenas with the First Amendment... 13
 - C. CoStar Has Not Met the “Sony Plus” Standard Required by the First Amendment. 15
- V. CONCLUSION 18

TABLE OF AUTHORITIES

Cases

A&M Records v. Napster, 239 F.3d 1004 (9th Cir. 2001)..... 17

Baker v. Selden, 101 U.S. 99 (1880) 11

Buckley v. Am. Constitutional Law Found., Inc., 525 U.S. 182 (1999) 7

Columbia Ins. Co. v. Seescandy.com, 185 F.R.D. 573 (N.D. Cal. 1999)..... 2, 3, 9

CoStar Group, Inc. v. LoopNet, Inc., 373 F.3d 544 (4th Cir. 2004) 4

Dastar Corp. v. Twentieth Century Fox Film Corp., 539 U.S. 23 (2003)..... 11

Dendrite Int’l, Inc. v. Doe No. 3, 775 A.2d 756 (N.J. Super. Ct. App. Div. 2001)..... passim

Doe v. 2TheMart, 140 F. Supp. 2d 1088 (W.D. Wash. 2001)..... 8, 9

Doe v. Cahill, 884 A.2d 451 (Del. 2005) 2, 10, 13

Eldred v. Ashcroft, 537 U.S. 186 (2003) 13

Field v. Google Inc., 412 F. Supp. 2d 1106 (D. Nev. 2006) 16

Gibson v. Florida Legislative Investigative Comm’n, 372 U.S. 539 (1963) 6

Highfields Capital Mgmt. L.P. v. Doe, 385 F. Supp. 2d 969 (N.D. Cal. 2004)..... passim

In re Charter Communications, Inc., Subpoena Enforcement Matter, 393 F.3d 771
(8th Cir. 2005) 8

Kelly v. Arriba Soft Corp., 336 F.3d 811 (9th Cir. 2003)..... 4

Lamont v. Postmaster General, 381 U.S. 301 (1965) 1, 7

Martin v. Struthers, 319 U.S. 141 (1943)..... 7

McIntyre v. Ohio Elections Comm’n, 514 U.S. 334 (1995) 1, 6

NAACP v. Alabama ex rel. Patterson, 357 U.S. 449 (1958)..... 1, 7

New York Times v. United States, 403 U.S. 713 (1971)..... 1

O’Grady v. Superior Court, 2006 Cal. App. LEXIS 802 (Cal. Ct. App. 2006) 1

Online Policy Group v. Diebold Inc., 337 F. Supp. 2d 1195 (N.D. Cal. 2004) 12, 17

Parker v. Google, Inc., 422 F. Supp. 2d 492 (E.D. Pa. 2006)..... 4

Perfect 10 v. Google, Inc., 416 F. Supp. 2d 828 (N.D. Cal. 2006) 1, 4, 16

Recording Indus. Ass’n of Am. v. Univ. of N.C. at Chapel Hill, 367 F. Supp. 2d 945
(M.D.N.C. 2005) 15

1 **I. INTRODUCTION AND SUMMARY OF ARGUMENT**

2 Almost a decade ago, the Supreme Court affirmed that First Amendment protections
3 enshrined in the Constitution must be safeguarded online as strongly as offline. *See Reno v. ACLU*,
4 521 U.S. 844, 870 (1997). These protections not only encompass the fundamental right to speak
5 freely and anonymously *Watchtower Bible & Tract Soc'y of N.Y., Inc. v. Vill. of Stratton*, 536 U.S.
6 150 (2002); *Reno v. ACLU*; *McIntyre v. Ohio Elections Comm'n*, 514 U.S. 334 (1995), the right to
7 a free press, *New York Times v. United States*, 403 U.S. 713 (1971); *O'Grady v. Superior Court*,
8 2006 Cal. App. LEXIS 802, 89-94 (Cal. Ct. App. 2006), and the right to freely and anonymously
9 associate, *NAACP v. Alabama ex rel. Patterson*, 357 U.S. 449, 462 (1958), but also the right to
10 read, watch, and listen anonymously. *See Stanley v. Georgia*, 394 U.S. 557 (1969); *Lamont v.*
11 *Postmaster General*, 381 U.S. 301 (1965).

12 By requesting the wholesale identification of each and every alleged “downloader” who has
13 ever so-much-as viewed a CoStar photo on the LoopNet system, CoStar seeks to eviscerate these
14 constitutional rights based on nothing more than mere speculation. Such demands cannot stand in
15 the face of the constitutional protections afforded to online users. No court has ever held that
16 simply viewing a webpage results in copyright infringement. In fact, the relevant case law treats
17 incidental copies created when an Internet user simply browses a webpage as non-infringing.
18 *Perfect 10 v. Google, Inc.*, 416 F. Supp. 2d 828, 852 n.17 (N.D. Cal. 2006) (concluding that copies
19 created by a web browser in the course of displaying web pages are likely covered by fair use).

20 CoStar’s contrary position would have startling results. If simply viewing a webpage,
21 clicking a link, or forwarding a link subjects one to identification under 17 U.S.C. § 512(h), then
22 any copyright holder could issue a 512(h) subpoena to any website that contained an unauthorized
23 copy of its content and demand to know each and every user who happen to have looked at it, even
24 if those users came upon the work completely by accident or innocently. The First Amendment and
25 due process forbid such invasions of privacy.

26 The chilling effects of such a precedent would be massive: at a minimum, email recipients
27 who wish to preserve their anonymity would have to avoid opening or forwarding links to a
28 website unless they have first made absolutely certain that the website does not contain an

1 unlicensed copyrighted work—an impossible task in many if not all cases—or risk finding
2 themselves unwittingly the target of a 512(h) subpoena. Even more frightening would be the loss of
3 anonymity for users merely browsing a web page. Those users would be caught in a Catch-22: not
4 knowing what images were on the web page until they loaded it up on their computer and once
5 they loaded the page, being subject to identification under a 512(h) subpoena if the images later
6 turned out to be infringing. Such an interpretation of 512(h) cannot withstand scrutiny under the
7 First Amendment’s protections for anonymous communication.

8 Nor is it the outcome Congress intended when it passed section 512(h). Section 512(h) was
9 not designed to be a statutory subpoena provision to help copyright holders gather general evidence
10 of suspected illegal conduct in order to build and prosecute a case of copyright infringement.
11 Rather, section 512(h) was intended to accomplish something more narrow – to assist in the
12 identification of a defendant against whom the copyright holder *already has evidence* of a
13 copyright violation and merely lacks the requisite personally identifying information on which to
14 fill out the complaint and serve it. CoStar’s overreaching use of 512(h) here goes far beyond this
15 Congressional intent and must be rejected.

16 These limitations—and CoStar’s disregard for them—underscore the need for clear
17 procedural safeguards on the 512(h) subpoena power. Such safeguards have already been
18 established in a variety of analogous contexts. Courts faced with similar expedited discovery
19 requests in defamation cases, for example, have shielded anonymous speakers and preserved their
20 First Amendment rights by requiring plaintiffs to demonstrate that their claims are valid and that
21 they have suffered a legally recognizable harm *before* the court will allow disclosure of the
22 speaker’s anonymity. *Doe v. Cahill*, 884 A.2d 451 (Del. 2005); *Dendrite Int’l, Inc. v. Doe No. 3*,
23 775 A.2d 756, 760-61 (N.J. Super. Ct. App. Div. 2001); *Highfields Capital Mgmt. L.P. v. Doe*, 385
24 F. Supp. 2d 969 (N.D. Cal. 2004); *Columbia Ins. Co. v. Seescandy.com*, 185 F.R.D. 573, 578 (N.D.
25 Cal. 1999). Similar procedural protections have also been implemented by statute in many states.
26 *See* Cal. Civ. Proc. Code § 425.16 (West 2006) (California SLAPP law).

27 Here, where pre-litigation discovery also threatens constitutionally-protected online
28 activity, the Court should do the same. Specifically, the court should consider (1) whether the

1 movant has demonstrated that it has viable claims, (2) the specificity of the discovery request, (3)
2 the existence of alternative means of discovery, (4) whether the movant has attempted to notify the
3 alleged infringer of pendency of the identification proceeding, and (5) the magnitude of the
4 movant’s need for the information. *See Dendrite*, 775 A.2d at 760-61; *Sony Music Entmn’t v. Does*
5 *1-40*, 326 F. Supp. 2d 556, 565 (S.D.N.Y. 2004) (“*Sony*”); *Columbia Ins. Co.* 185 F.R.D. at 578-
6 80. In addition, the Court should “assess and compare the magnitude of the harms that would be
7 caused to the competing interests by a ruling in favor of [movant] and by a ruling in favor of [the
8 anonymous individuals].” *Highfields*, 385 F. Supp. 2d at 976. Careful consideration of these factors
9 will ensure that constitutional rights are protected while still allowing copyright owners who show
10 legitimate harm to their interests to proceed and unmask the anonymous user.

11 EFF respectfully requests that the Court adopt the above test to evaluate CoStar’s 512(h)
12 subpoena in this case and thereafter rule against CoStar’s Motion based on the facts at hand.

13 **II. INTERESTS OF AMICUS**

14 *Amicus Electronic Frontier Foundation* (“EFF”) is a member-supported non-profit public
15 interest organization working to protect fundamental rights regardless of technology; to educate the
16 press, policymakers and the general public about civil liberties issues related to technology; and to
17 act as a defender of those liberties. EFF currently has over 11,000 contributing members
18 nationwide, and over 50,000 subscribers to EFFector, its email newsletter. EFF is particularly
19 concerned with protecting the rights of individuals to speak and read anonymously, on the Internet
20 or otherwise, and regularly advises and defends individuals around the country whose free speech
21 rights are threatened. EFF was also a named plaintiff in the seminal Internet free speech case of
22 *Reno v. ACLU*, 521 U.S. 844 (1997), and has appeared as *amicus curiae* in a variety of cases
23 raising the proper standards governing the use of subpoenas to compromise anonymity online.

24 **III. BACKGROUND**

25 Both Movants CoStar Group, Inc. and CoStar Realty Information, Inc. (collectively,
26 “CoStar”) and Respondent LoopNet, Inc. (“LoopNet”) are providers of real estate information.
27 CoStar has created a large database of real estate information, including photographs, which it
28 makes available to subscribers via the Internet. *CoStar Group, Inc. v. LoopNet, Inc.*, 373 F.3d 544,

1 546 (4th Cir. 2004). LoopNet, by contrast, is an “Internet service provider (‘ISP’) whose website
2 allows subscribers, generally real estate brokers, to post listings of commercial real estate on the
3 Internet.” *Id* at 547. LoopNet essentially offers a “do it yourself” service; instead of posting its own
4 real estate information, it allows its subscribers to do so on their own. *See* Warthen Decl. in Opp. to
5 Costar’s Mot. to Compel ¶ 6. LoopNet subscribers can upload and save profiles of properties for
6 rent or sale. *Id.* ¶ 7. Users can query for properties within requested parameters (location, price,
7 etc.) and receive listings of different property profiles. Users can also sign up to receive automatic
8 e-mails containing such queried listings and links to property profiles when they become available.
9 These profiles may include thumbnail pictures of the properties (which can be enlarged), including
10 pictures for which CoStar allegedly holds the copyrights (“CoStar pictures”).

11 When e-mails containing links to property photographs are forwarded through LoopNet’s
12 various e-mail services, the actual photographs are not copied or sent. Instead, either a hyperlink or
13 an “in-line link” to the photographs is sent in the e-mail message. *See* Warthen Decl., ¶ 15. These
14 “in-line links” are not copyrighted works and they are certainly not CoStar’s property. Rather, they
15 are Universal Resource Locations (commonly known as a URLs) that give the user the location of
16 the photograph associated with the property mentioned in the email. *Id.* The link “instructs” the
17 user’s e-mail program automatically to “retrieve the linked-to image from the source website and
18 display it on the user's screen, but does so without leaving the linking document.” *Kelly v. Arriba*
19 *Soft Corp.*, 336 F.3d 811, 816 (9th Cir. 2003).

20 After receiving such an e-mail, or when browsing through LoopNet’s website, a user’s
21 computer system may automatically cache the images displayed on the screen. A browser cache is
22 “a temporary storage tool,” *Parker v. Google, Inc.*, 422 F. Supp. 2d 492, 495 (E.D. Pa. 2006),
23 designed to “speed up the loading of Internet displays [by] stor[ing] a copy of the page on the
24 computer's hard drive When the user later returns to a previously visited webpage, the browser
25 retrieves the cached file to display the webpage instead of retrieving the file from the Internet. By
26 retrieving the page from the cache, instead of the Internet, the browser can display the page more
27 quickly.” Ty E. Howard, *Don’t Cache out your Case*, 19 BERKELEY TECH. L.J. 1227, 1229-1230
28 (2004). A web cache acts automatically, without any user input. *Perfect 10 v. Google, Inc.*, 416 F.

1 Supp. 2d at 852 (“Local browser caching basically consists of a viewer's computer storing
2 automatically the most recently viewed content of the websites the viewer has visited. It is an
3 automatic process of which most users are unaware.”); *see also United States v. Tucker*, 305 F.3d
4 1193, 1198 n.7 (10th Cir. 2002) (“The Web browser automatically caches such images; no act is
5 required of the user. The purpose of caching is to allow already-visited pages to forego the
6 necessity of loading pictures and thus allow visits to these pages to be processed much faster.”).

7 In 1999, CoStar sued LoopNet for direct and indirect copyright infringement. *See Wilson*
8 Decl. in Opp. To Costar’s Mot. to Compel ¶ 5. The Fourth Circuit Court of Appeals rejected
9 CoStar’s direct copyright infringement claims after the parties settled their other claims. *Wilson*
10 Decl. ¶ 6-7. Having failed in its copyright suit against LoopNet, CoStar now asserts, at least
11 implicitly, that it intends to sue LoopNet users directly, although CoStar's track record provides
12 some reason to doubt this assertion. Toward that end, it is demanding identifying information for
13 those subscribers, relying on 17 U.S.C. § 512(h), the subpoena provision of the Digital Millennium
14 Copyright Act (“DMCA”). Specifically, the subpoena seeks any identifying information from
15 LoopNet on users who have “uploaded” or “downloaded” any CoStar pictures. CoStar defines
16 “uploading” as “posting, submitting, providing, transmitting or copying to LoopNet...” and defines
17 “downloading” as:

18 copying, transferring, or obtaining from any server owned or operated by LoopNet a
19 digital copy of one or more of CoStar’s photographs, including, but not limited to,
20 in connection with use of (a) the LoopNet listing service, or (b) any LoopNet
21 product or service that utilizes photographs from the LoopNet listing service,
22 including, but not limited to, (i) the LoopNet Prospect List lead generation service,
23 (ii) the LoopNet Email Alert service, (iii) the LoopNet Personalized ListingsLink
24 service, (iv) the LoopNet Customer Marketing Email service, and (v) any LoopNet
25 Saved Property Folders.

26 CoStar Subpoena Schedule A. CoStar subsequently characterized downloaders as “individuals who
27 had further reproduced or distributed CoStar’s copyrighted photographs through the LoopNet
28 system.” Mot. to Compel at 7. Loopnet has provided information regarding uploaders, but has
asserted that it does not possess information that would enable it to identify any alleged
downloaders.

1 **IV. ARGUMENT**

2 **A. The Court Must Balance CoStar’s Litigation Interests Against the Anonymous**
3 **Downloaders’ Free Speech Interests.**

4 As a copyright owner, CoStar has a legitimate interest in enforcing its rights against those
5 who infringe its interests. However, while CoStar’s motion claims that it seeks only “information
6 concerning infringing subscribers,” Mot. to Compel at 7, its subpoena demands that Loopnet
7 provide information identifying virtually anyone who has ever received, forwarded or clicked on a
8 link to a web page that happened, at one time, to contain a thumbnail version of a photograph as to
9 which CoStar allegedly holds the copyright. CoStar Subpoena Schedule A. This broad language
10 thus attempts to capture a wide range of online activity, including the activity of anonymous online
11 speakers and readers of LoopNet’s site. As such, the Court must evaluate CoStar’s right to this
12 information against the constitutional protections afforded these speakers and readers under the
13 First Amendment.

14 **1. Efforts To Use The Power Of The Courts To Pierce Anonymity Are**
15 **Subject To A Qualified Privilege.**

16 **a. The First Amendment protects anonymous online**
17 **communication.**

18 Courts have long recognized protection under the First Amendment for the right to engage
19 in anonymous communication—to speak, read, listen, and/or associate anonymously—as
20 fundamental to a free society. The Supreme Court has consistently defended such rights in a variety
21 of contexts. “Anonymity is a shield from the tyranny of the majority ... [that] exemplifies the
22 purpose [of the First Amendment:] to protect unpopular individuals from retaliation . . . at the hand
23 of an intolerant society.” *McIntyre v. Ohio Elections Comm’n*, 514 U.S. at 357 (holding that an
24 “author’s decision to remain anonymous, like other decisions concerning omissions or additions to
25 the content of a publication, is an aspect of the freedom of speech protected by the First
26 Amendment”); *Gibson v. Florida Legislative Investigative Comm’n*, 372 U.S. 539, 544 (1963)
27 (“[I]t is ... clear that [free speech guarantees] ... encompass[] protection of privacy of
28

1 association”).¹ See also *Stanley v. Georgia*, 394 U.S. at 564 (“the Constitution protects the right to
2 receive information and ideas.”); *Schneider v. Smith*, 390 U.S. 17, 24-25 (1968) (First Amendment
3 forbids “abridging’ freedom of speech,” by “prob[ing] of *reading habits*, political philosophy,
4 beliefs, and attitudes on social and economic issues”) (emphasis added); *Lamont v. Postmaster*
5 *General*, 381 U.S. 301, 308 (1965) (BRENNAN, J., concurring) (“The dissemination of ideas can
6 accomplish nothing if otherwise willing addressees are not free to receive and consider them. It
7 would be a barren marketplace of ideas that had only sellers and no buyers.”); *Martin v. Struthers*,
8 319 U.S. 141, 143 (1943) (“The right of freedom of speech and press . . . embraces the right to
9 distribute literature, and necessarily protects the right to receive it.”) (citation omitted); Julie
10 Cohen, *A Right to Read Anonymously: A Closer Look at “Copyright Management” In Cyberspace*,
11 28 CONN. L. REV. 981 (1996) (“Cohen”) (summarizing First Amendment protections for
12 anonymity and concluding “that the close interdependence between receipt and expression of
13 information and between reading and freedom of thought make recognition of such a right sound
14 constitutional policy.”).

15 **b. Anonymous online communication is subject to a qualified**
16 **privilege.**

17 Because the First Amendment protects anonymous communication (including the right to
18 read, watch, and listen anonymously), efforts to use the power of the courts to pierce such
19 anonymity are subject to a qualified privilege. Courts must “be vigilant . . . [and] guard against
20 undue hindrances to . . . the exchange of ideas.” *Buckley v. Am. Constitutional Law Found., Inc.*,
21 525 U.S. 182, 192 (1999). This vigilant review “must be undertaken and analyzed on a case-by-
22 case basis,” where the court’s “guiding principle is a result based on a meaningful analysis and a
23 proper balancing of the equities and rights at issue.” *Dendrite*, 775 A.2d at 760-61.

24 _____
25 ¹ See also *Talley v. California*, 362 U.S. 60, 64 (1960) (finding a municipal ordinance requiring
26 identification on hand-bills unconstitutional, and noting that “anonymous pamphlets, leaflets,
27 brochures and even books have played an important role in the progress of mankind.”); *Patterson*,
28 357 U.S. 449 (compelled identification violated group’s members’ right to remain anonymous;
“[i]nviolability of privacy in group association may in many circumstances be indispensable to
preservation of freedom of association.”).

1 Moreover, that review must take place whether the communication in question takes the
2 form of political pamphlets, Internet postings, or email. *Reno v. ACLU*, 521 U.S. at 870 (there is
3 “no basis for qualifying the level of First Amendment protection that should be applied to” the
4 Internet); *see also, e.g., Doe v. 2TheMart*, 140 F. Supp. 2d 1088, 1093 (W.D. Wash. 2001) (“The
5 right to speak anonymously extends to speech via the Internet. Internet anonymity facilitates the
6 rich, diverse, and far ranging exchange of ideas.”); *Sony*, 326 F. Supp. 2d at 562 (“The Internet is a
7 particularly effective forum for the dissemination of anonymous speech.”); *Cohen* at 1005 (arguing
8 that protection of anonymous reading is especially crucial online, where “reading” is an interactive
9 and “message-shaping” enterprise).

10 And that review is particularly important where, as here, discovery takes place outside of
11 any actual litigation, based on nothing more than suspicions of infringement. Section 512(h)
12 empowers anyone alleging “unauthorized” use of a copyrighted work to obtain from a district court
13 clerk a pre-litigation judicial subpoena demanding the name, address, telephone number, and other
14 identifying information of any Internet user. That subpoena issues with no judicial oversight, no
15 ongoing or even anticipated litigation, and no required notice to the person whose identity is to be
16 disclosed.² No clerk, much less a judge, evaluates the substance or veracity of the assertions; if the
17 paperwork is submitted in order, the clerk must sign the subpoena for delivery to an Internet
18 Service Provider (ISP). Unless courts apply the correct balancing test to evaluate the claims
19 underlying the subpoena, any copyright owner would be unilaterally empowered to compromise an
20 individual’s privacy and anonymity on the Internet.

21 **2. The Qualified Privilege Requires the Evaluation Of Multiple Factors**
22 **Prior to Subpoena Enforcement**

23 A qualified privilege to remain anonymous is not an absolute privilege. Like any other
24 litigant, CoStar has a right to seek information necessary to pursue reasonable and meritorious
25 litigation. The issue, then, is the appropriate balance between the competing interests of CoStar and
26

27 ² The lack of actual case or controversy as a predicate for issuance of the subpoena also raises
28 serious Article III concerns as to the constitutionality of section 512(h). *See In re Charter*
Communications, Inc., Subpoena Enforcement Matter, 393 F.3d 771, 783 (8th Cir. 2005).

1 the anonymous readers and speakers it seeks to unmask. *See Sony*, 326 F. Supp. 2d at 565
2 (“Against the backdrop of First Amendment protection for anonymous speech, courts have held
3 that civil subpoenas seeking information regarding anonymous individuals raise First Amendment
4 concerns”); *Dendrite*, 775 A.2d at 771 (strict procedural safeguards must be imposed on subpoenas
5 to ensure that “plaintiffs do not use discovery procedures to ascertain the identities of unknown
6 defendants in order to harass, intimidate or silence critics in the public forum opportunities
7 presented by the Internet”); *Columbia Ins. Co.*, 185 F.R.D. at 578 (when issuing subpoenas in Doe
8 cases, plaintiff’s desire to seek redress for injury must be balanced against the legitimate and
9 valuable right to participate in online forums anonymously or pseudonymously).

10 The tension between the qualified privilege to communicate anonymously and the interest
11 of a plaintiff in obtaining information necessary to pursue litigation has been considered by a
12 variety of federal and state courts over the past several years. *Id*; *see also e.g., 2TheMart.com*, 140
13 F. Supp. 2d 1088 (granting, on First Amendment grounds, motion to quash subpoena to ISP
14 seeking identification of anonymous messages critiquing various parties). These courts have
15 employed a variety of multi-part balancing tests to decide whether or not to compel the
16 identification of an anonymous Internet communicator.

17 In one of the first cases to address the issue, *Columbia Ins. Co.*, this Court balanced
18 plaintiff’s desire to seek redress for injury to its trademarks against the legitimate and valuable
19 right to participate in online forums anonymously or pseudonymously. The Court required the
20 plaintiff to (1) identify the missing party with sufficient specificity that the court could determine
21 whether the defendant could be sued in federal court; (2) make a good faith effort to communicate
22 with the anonymous defendants and to provide them with notice that the suit had been filed against
23 them – thus assuring them an opportunity to defend their anonymity; and (3) demonstrate that it
24 had viable claims against such defendants. 185 F.R.D. at 579.

25 More recently, in a trademark and defamation action (among other claims), this Court held
26 that the protected interest in speaking anonymously requires a plaintiff to adduce competent
27 evidence that “if unrebutted, tend[s] to support a finding of each fact that is essential to a given
28 cause of action.” *Highfields*, 385 F. Supp. 2d at 975. If the first component of the test is met, the

1 Court held that it should then “assess and compare the magnitude of the harms that would be
2 caused to the competing interests by a ruling in favor of plaintiff and by a ruling in favor of
3 defendant,” and enforce the subpoena only if its issuance “would cause relatively little harm to the
4 defendant’s First Amendment and privacy rights [and] is necessary to enable plaintiff to protect
5 against or remedy serious wrongs.” *Id.* at 976.

6 Two state appellate courts—still the only appellate courts to address the issue—have
7 adopted similar tests. In *Dendrite*, a New Jersey appeals court required the plaintiff in a defamation
8 action against Doe defendants to (1) use the Internet to notify the accused of the pendency of the
9 identification proceeding and to explain how to present a defense; (2) quote verbatim the allegedly
10 actionable online speech; (3) allege all elements of the cause of action; (4) present evidence
11 supporting the claim of violation; and; “[f]inally, assuming the court concludes that the plaintiff
12 has presented a prima facie cause of action, the court must balance the defendant’s First
13 Amendment right of anonymous free speech against the strength of the prima facie case presented
14 and the necessity for the disclosure of the anonymous defendant’s identity to allow the plaintiff to
15 properly proceed.” 775 A.2d at 761.

16 And in *Doe v. Cahill*, 884 A.2d 451 (Del. 2005), the Delaware Supreme Court held that,
17 after making reasonable efforts to notify the anonymous defendant, “to obtain discovery of an
18 anonymous defendant’s identity under the summary judgment standard, a defamation plaintiff
19 ‘must submit sufficient evidence to establish a prima facie case for each essential element of the
20 claim in question.’” *Id.* at 463.

21 Decisions in copyright infringement actions against Doe defendants are no exception to this
22 trend, nor should they be. The First Amendment does not protect anonymous individuals against
23 suit where there is clear proof that they have infringed copyrights unlawfully. However, allegations
24 of copyright infringement are inherently no more reliable than allegations of trademark
25 infringement, defamation, or other types of unprotected speech. Thus, in *Sony*, the court weighed
26 five factors prior to enforcing a Rule 45 subpoena against anonymous defendants in a copyright
27 case: “(1) [the existence of] a concrete showing of a prima facie claim of actionable harm ... (2)
28 specificity of the discovery request ... (3) the absence of alternative means to obtain the

1 subpoenaed information ... (4) a central need for the subpoenaed information to advance the claim
2 ... and (5) the party's expectation of privacy" prior to enforcement. *Sony*, 326 F. Supp. 2d at 564-
3 65.

4 **B. The Complexities of Copyright Law and the Potential for Misuse of Section**
5 **512(h) Requires Application of A "Sony Entertainment Plus" Standard**

6 **1. The Complexities of Copyright Law and the Potential for Misuse of**
7 **Section 512(h) raise serious concerns under the First Amendment**

8 Because of copyright law's complexity and the fact that Section 512(h) subpoenas issue
9 without any judicial review, it is entirely possible that information will be released through these
10 procedures against innocent non-infringers, thus irreparably abrogating their rights to privacy and
11 anonymity. This is especially true where the innocent party has made fair use of the copyrighted
12 material, only used the underlying ideas in the material, or used material in the public domain. *See*
13 17 U.S.C. § 107; *Baker v. Selden*, 101 U.S. 99, 103-104 (1880) (holding ideas within copyrighted
14 works unprotectable); *Dastar Corp. v. Twentieth Century Fox Film Corp.*, 539 U.S. 23, 31 (2003)
(affirming right to distribute public domain works as supportive of the Copyright Act's purpose).

15 In fact, there have already been instances of misuse, overreaching, and mistakes in various
16 sections of the DMCA, including Section 512(h) subpoenas, Section 512(c)(3)(A) notices, or their
17 equivalent:

- 18 • **Plain Errors:** In 2003, the Recording Industry Association of America (RIAA)
19 sent a DMCA notice to Penn State's Department of Astronomy and
20 Astrophysics, accusing the university of unlawfully distributing songs by the
21 musician Usher. As it turned out, RIAA had mistakenly identified the
22 combination of the word "Usher" (identifying faculty member Peter Usher) and
23 an a cappella song performed by astronomers about a gamma ray as an instance
24 of infringement. In apologizing, RIAA noted that its "temporary employee" had
25 made an error. *See McCullagh, RIAA Apologizes for Threatening Letter*, CNET
26 News, May 12, 2003, http://news.com.com/2100-1025_1001095.html.
- 27 • **Uncopyrightable Facts:** In 2002, Wal-Mart sent a Section 512(h) subpoena,
28 along with a 512(c) notice, to a comparison-shopping website that allows
consumers to post prices of items sold in stores, claiming incorrectly that its
prices were copyrighted. Wal-Mart sought the identity of the consumer who had
anonymously posted information about an upcoming sale. Other retailers,
including Kmart, Jo-Ann Stores, OfficeMax, Best Buy, and Staples, also served
512(c) notices on the website based on the same theory. Eventually, all the
retailers backed off these claims, but not until after the subpoena and take-down
notices had been issued. *See McCullagh, Wal-mart Backs Away from DMCA
Claim*, CNET News, Dec. 5, 2002, <http://news.com.com/2100-1023-976296.html>.

- 1 ● **Public Domain Materials:** The Internet Archive (<http://www.archive.org>) is a
2 well-known website containing numerous public domain films, including parts
3 of the historic Prelinger collection. Many of these films have numerical file
4 names. A purported copyright owner sent a DMCA Section 512 notice to the
5 Internet Archive in connection with films 19571.mpg and 20571a.mpg. The
6 sender mistook the Prelinger public domain films for the copyrighted submarine
7 movie “U-571.” *See* Chilling Effects Clearinghouse: Universal Studios Stumbles
8 on Internet Archive's Public Domain Films, <http://www.chillingeffects.org/notice.cgi?NoticeID=595> (last visited June 19,
9 2006); Chilling Effects Clearinghouse: Internet Archive: Our Films are Public
10 Domain, <http://www.chillingeffects.org/responses/notice.cgi?NoticeID=597> (last
11 visited June 19, 2006).
- 12 ● **Fair Use:** In 2003, electronic voting machine manufacturer Diebold, Inc. sent a
13 DMCA Section 512 notice to several ISPs claiming that posting of embarrassing
14 internal emails on voting activists’ websites was a copyright violation and must
15 be taken down immediately. A court later determined that these postings were a
16 fair use of the copyrighted materials and that the DMCA notice was an abuse of
17 the legal process by Diebold. *See Online Policy Group v. Diebold Inc.*, 337
18 F. Supp. 2d 1195 (N.D. Cal. 2004).

19 As this sampling suggests, when copyright holders have the power to issue subpoenas and
20 take-down notices absent judicial review, the potential for abuse of Section 512 rises significantly.
21 It is for this very reason that Congress intended 512(h) to be a subpoena solely for the purpose of
22 identifying the perpetrator of a *known* case of infringement—not as a fishing expedition to unmask
23 Internet users in an attempt to discover possible infringement or intimidate those users.

24 Moreover, Section 512(h)’s modest prerequisites offer very little protection to Internet
25 users. Section 512(h) does not require the subpoenaing party to demonstrate that the copyrights
26 allegedly at issue are enforceable; the requester of a subpoena need only state a “good-faith belief”
27 of infringement in the underlying 512(c) notice, and is not expressly required to undertake any due
28 diligence, such as actual review of the suspicious files. And, although a Section 512(h) subpoena is
signed under penalty of perjury, this affirmation applies not to the allegations of infringement but
rather only to the identification of the “purpose” of the requester and the uses to which the
information will be put. 17 U.S.C. § 512(h)(2)(C).³

³ In contrast, “John Doe” subpoenas under Fed. R. Civ. P. 45 require a plaintiff to first file suit and then request expedited third-party discovery directly from the Court, allowing for judicial review of the request and its merits. This is further contrasted with the typical third-party subpoena process, which can only proceed after the named defendant has answered the complaint and the parties have engaged in the requisite Rule 26(f) conference.

1 To combat such misuse, courts must provide a safeguard against improper disclosure when
2 such subpoenas are challenged. Due process dictates that the accused should not be forced to
3 undergo the harm of losing their anonymity unless and until the subpoenaing party has submitted at
4 least some competent evidence as to the viability of their claims—including the ability to survive
5 self-evident defenses such as fair use. Once an online user’s anonymity and privacy have been
6 eviscerated, they cannot be repaired or the user made whole.

7 **2. The “Sony Plus” test properly balances 512(h) subpoenas with the First**
8 **Amendment**

9 While all of the aforementioned courts balanced legal rights and discovery mechanisms
10 with First Amendment protections using slightly different tests, a strong unifying principle is clear:
11 a plaintiff must show that she has a viable case and no other avenue of vindicating her rights before
12 a court will allow her to pierce an online user’s veil of anonymity. In the instant case, the Court
13 should also follow this principle and evaluate 512(h) subpoenas using a test drawn from the
14 strongest and most analogous decisions.

15 For example, the *Sony* test offers a useful starting point for balancing the countervailing
16 constitutional and litigation interests in a copyright infringement action involving a potential Doe
17 defendant, but fails to account for an additional crucial factor: the likelihood that the disputed use
18 is non-infringing. Copyright law, by its nature, necessarily implicates core First Amendment issues
19 because it imposes significant restrictions directly on public debate and the expression of ideas. For
20 that reason, copyright law has “built-in First Amendment accommodations” including the fair use
21 doctrine and the idea/expression distinction. *Eldred v. Ashcroft*, 537 U.S. 186, 217 (2003). These
22 and other limitations on copyright protections require case-by-case determinations based on the
23 careful review of such complex and subtle factors as the amount of the work used and the effect on
24 the market for a work. *See* 17 U.S.C. § 107 (listing the four main factors to be considered in a fair
25 use analysis).

26 In addition to *Sony*, this court should also consider adopting elements of the tests articulated
27 in *Doe v. Cahill* and *Highfields*. These courts raised serious due process concerns over the lack of
28 notice given to the anonymous user whose identity is at issue and the possibility that plaintiffs’

1 claims might not survive on summary judgment. *Doe v. Cahill*, 884 A.2d at 460 (“[T]he summary
2 judgment standard is the appropriate test by which to strike the balance between a defamation
3 plaintiff’s right to protect his reputation and a defendant’s right to exercise free speech
4 anonymously.”); *Highfields*, 385 F. Supp. 2d at 975 (“Because of the importance and vulnerability
5 of those [constitutional] rights, ... the plaintiff [must] persuade the court that there is a real
6 evidentiary basis for believing that the defendant has engaged in wrongful conduct that has caused
7 real harm to the interests of the plaintiff”). Here, where certain defenses such as fair and other
8 non-infringing uses might be self-evident, the Court should require that the issuer of a 512(h)
9 subpoena articulate the validity and strength of their claims, including addressing these defenses.⁴
10 If the petitioner can meet this threshold element, the court should consider the specificity of the
11 discovery request, the existence of alternative means of discovery, whether the petitioner has
12 attempted to notify the alleged infringer of pendency of the identification proceeding, and the
13 magnitude of the petitioner’s need for the information. Finally, the Court should “assess and
14 compare the magnitude of the harms that would be caused to the competing interests by a ruling in
15 favor of plaintiff and by a ruling in favor of defendant.” *Highfields*, 385 F. Supp. 2d at 976.

16 Copyright holders should have little difficulty meeting this test if, as section 512(h)
17 contemplates, they already have investigated and gathered evidence sufficient to allege copyright
18 infringement, and seek only information identifying the infringer. 17 U.S.C. § 512(h). Section 512
19 is not a subpoena to identify facts relating to the *conduct* of an alleged infringer, but rather to
20 supply information sufficient to *identify* a known infringer. These limitations in Section 512(h) are
21 critically important, not only because they are consistent with the plain language of the statute itself
22 but also because to read 512(h) as broader than this would abrogate important First Amendment
23 values. If copyright holders lack information sufficient to conduct that prior investigation, their
24 appropriate remedy is to file a complaint naming John Doe defendant(s) and then seek discovery of
25
26

27
28 ⁴ While the burden of addressing defenses typically falls on the defendant, here it must fall on the
movant unless the defendant is contacted and chooses to appear.

1 both activity and identities under normal discovery rules.⁵

2 The above test strikes the right balance between the interests of copyright owners and
3 anonymous users online. Application of the test will do much to mitigate the risk of improperly
4 invading First Amendment “rights that are fundamental and fragile -- rights that the courts have a
5 special duty to protect against unjustified invasion.” *Highfields*, 385 F. Supp. 2d at 975. And, it will
6 impose only a minimal additional burden on copyright holders who have already done a proper
7 pre-litigation investigation. Given the importance of the constitutional interests at stake, the narrow
8 scope of the 512(h) subpoena power, and the potential misuse by copyright owners, this Court
9 should ask no less.

10 **C. CoStar Has Not Met the “Sony Plus” Standard Required by the First**
11 **Amendment.**

12 CoStar’s subpoena and Motion fall far short of meeting the “Sony Plus” test. First and
13 foremost, CoStar has not come forward with evidence sufficient to demonstrate that it has viable
14 copyright claims against any of the “downloaders” whose identities it seeks in its overbroad 512(h)
15 subpoena.

16 In targeting “LoopNet subscribers who have reproduced or disseminated CoStar’s
17 copyrighted photographs,” CoStar’s subpoena essentially seeks to identify three categories of
18 visitors to LoopNet’s website: (1) those who uploaded CoStar photographs (“uploaders”); (2)
19 individuals who simply viewed the page on which such photographs appeared (“downloaders”);
20 and (3) individuals who used the “Customer Marketing Email” feature to send email messages that
21 included links leading to pages on which such photographs appeared (“emailers”). LoopNet Mot. at
22 9.

23 As to “uploaders,” LoopNet has already provided the information sought. LoopNet Opp. at
24 8. As to “downloaders,” CoStar has failed to establish a viable claim against individuals who
25 simply visit a LoopNet web page and thereby “download” its associated images. This is because

26 _____
27 ⁵ Indeed, numerous music copyright holders have used this procedure in a widely-publicized
28 lawsuit campaign against thousands of alleged music file-sharers. *See e.g., Elektra Entm’t Group, Inc. v. Does 1-9*, 2004 U.S. Dist. LEXIS 23560 (S.D.N.Y. 2004); *Sony*, 326 F. Supp. 2d 556.

1 the only copy made when viewing a photograph on LoopNet’s website is the automatic “cache”
2 copy made by his or her Internet browser. LoopNet Opp. at 12, n.11. As one California district
3 court recently concluded, to the extent these incidental copies are “reproductions” within the
4 meaning of the Copyright Act, they are excused by the fair use doctrine:

5 “[l]ocal browser caching basically consists of a viewer’s computer storing
6 automatically the most recently viewed content of the websites the viewer has
7 visited. It is an automatic process of which most users are unaware, and its use
8 likely is ‘fair.’ ... Local caching by the browsers of individual users is
9 noncommercial, transformative, and no more than necessary to achieve the
10 objectives of decreasing network latency and minimizing unnecessary bandwidth
11 usage (essential to the internet). It has a minimal impact on the potential market for
12 the original work, especially given that most users would not be able to find their
13 own local browser cache, let alone locate a specific cached copy of a particular
14 image.”

11 *Perfect 10 v. Google, Inc.*, 416 F. Supp. 2d at 852 n.17;⁶ *see also Field v. Google Inc.*, 412 F. Supp.
12 2d 1106, 1109 (D. Nev. 2006) (automatically cached images on Google’s commercial server were
13 fair uses).⁷

14 As to “emailers,” CoStar baldly asserts that “[e]ach LoopNet subscriber who sends an e-
15 mail listing containing a copyrighted CoStar photograph is an infringer.” CoStar Mot. at 11. As
16 LoopNet points out, however, the emails generated by the “Customer Marketing Email” and
17 “Email Alert” services do not “contain” photographs at all, but rather merely link back to Property
18 Profile files. Warthen Decl. at ¶ 15. CoStar has failed to come forward with evidence sufficient to
19 establish a viable copyright claim against LoopNet users based on these activities. As this Court
20 has previously held, merely providing a link does not trigger any direct infringement liability, as

21 ⁶ Moreover, at the Committee on the Judiciary Hearing on The Copyright Infringement Liability of
22 Online and Internet Service Providers (a precursor to passing Section 512 of the DMCA) on
23 September 4, 1997, in response to a questions from Senator Leahy: “[u]nder what circumstances, if
24 any, would an individual ‘browsing’ the Web be subject to liability for copyright infringement?”
25 Fritz Attaway, senior vice president of government relations and Washington general counsel of
the Motion Picture Association of America, one of the DMCA’s strongest proponents, responded:
“the simple act of ‘browsing,’ without more, would not create liability.”

26 ⁷ CoStar also vaguely asserts that other LoopNet features, such as the “Saved Properties Folder,”
27 result in reproductions of images owned by CoStar. As LoopNet points out, none of these features
28 relies on any further reproductions, but instead rely on URL links back to the original image stored
with the Property Profile. Warthen Decl. at ¶ 15. Accordingly, when “downloaders” use these
features, they are not making any further copies.

1 the activity does not invade any of the exclusive rights of a copyright owner. *See Online Policy*
2 *Group v. Diebold, Inc.*, 337 F. Supp. 2d at 1202 n.12 ("Hyperlinking per se does not constitute
3 direct copyright infringement because there is no copying."); *accord Ticketmaster Corp. v.*
4 *Tickets.com, Inc.*, CV 99-7654 HLH, 2000 WL 525390, at *2 (C.D. Cal. Mar. 27, 2000)
5 ("[H]yperlinking does not itself involve a violation of the Copyright Act ...since no copying is
6 involved.".)⁸

7 Because CoStar has failed to submit competent evidence supporting the viability of its
8 copyright claims, there is no need for the court to consider the remaining factors of the proposed
9 balancing test. That said, those factors also weigh against CoStar. As discussed by LoopNet,
10 CoStar's discovery request is not specific but rather a woefully over-inclusive fishing expedition.
11 Moreover, there is nothing in the record to suggest that CoStar has explored using alternative
12 means to identify potential infringers or even attempted, e.g., via a targeted web advertisement or
13 watermarking of their photos, to notify users of the risk of having their identity subpoenaed. As for
14 the extent of the need, absent viable claims it is difficult to identify an urgent need for the
15 identifying information. Finally, releasing the information requested would cause significant harm
16 to the anonymous users by forcing them to give up their anonymity and potentially face frivolous
17 litigation, in many cases as a result of nothing more than the innocent act of viewing a web page or
18 recommending the web page to an acquaintance or client.

19 ///

20 ///

21 ///

22 ///

23 ///

24
25 ⁸ CoStar here has also failed to establish any viable secondary liability claim against "emailers." In
26 order to make such a claim, CoStar would have to establish that the recipients of the emails directly
27 infringe CoStar's copyrights when they follow the link and view LoopNet web pages. *See A&M*
28 *Records v. Napster*, 239 F.3d 1004, 1013 n.2 (9th Cir. 2001) ("Secondary liability for copyright
infringement does not exist in the absence of direct infringement by a third party."). For the reasons
discussed above, viewing a web page, without more, does not infringe copyright. CoStar here has
failed to adduce any evidence of "something more" on the part of any LoopNet subscriber.

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

V. CONCLUSION

For the foregoing reasons, Amicus EFF respectfully requests that the Court adopt the “Sony Plus” test for evaluating subpoenas under Section 512(h) of the DMCA and, upon the current factual record, deny CoStar’s Motion to Compel.

DATED: June 20, 2006

Respectfully submitted,

ELECTRONIC FRONTIER FOUNDATION

By _____

Cindy A. Cohn (SBN 145997)
Jason M. Schultz (SBN 212600)
Corynne McSherry (SBN 221504)
454 Shotwell Street
San Francisco, CA 94110
Telephone: (415) 436-9333
Facsimile: (415) 436-9993

Attorneys for Amicus Curiae
ELECTRONIC FRONTIER FOUNDATION