RATIONALIZING INTERNET SAFE HARBORS

MARK A. LEMLEY*

Internet intermediaries – service providers, Web hosting companies, Internet backbone providers, online marketplaces, and search engines – process hundreds of millions of data transfers every day, and host or link to literally tens of billions of items of third party content. They can process and host that data instantaneously[1] only because they automate the process.

Some of this content is illegal. It may infringe copyrights, violate trademarks, disclose trade secrets, defame others, violate privacy rights, contain child pornography, or any of a host of other possible torts or crimes. In the last 12 years, both Congress and the courts have concluded that Internet intermediaries should not be liable for damages for a wide range of content posted or sent through their systems by another.[2] The reasoning behind these immunities is impeccable: if Internet intermediaries were liable every time someone posted problematic content on the Internet, the resulting threat of liability and

* William H. Neukom Professor, Stanford Law School; of counsel, Keker & Van Nest LLP. Thanks to Stacey Dogan, Eric Goldman, Paul Goldstein, Rose Hagan, Ed Lee, Fred von Lohmann, Phil Weiser, and participants in the Digital Broadband Migration conference at the University of Colorado School of Law for helpful comments. I currently represent or have in the past represented various Internet intermediaries, including Google, eBay, and Pacific Bell Internet Services. I also represent plaintiffs seeking redress for online harms in *Doe v. Ciolli*, among other cases. I emphasize that my opinions are my own, not those of my firm or my clients.

1. A search for the word "the" on Google on November 30, 2006 produced approximately 5.8 billion results and took 0.03 seconds. Google Search, The, http://www.google.com/search?hl=en&q=the&btnG=Google+Search (last visited Sept. 17, 2007).

2. *See generally* 15 U.S.C. § 1114(2)(B)-(C) (2000) (trademark); 17 U.S.C. § 512 (2000) (copyright); 47 U.S.C. § 230 (2000) (all causes of action other than intellectual property); Universal Commc'n Sys., Inc. v. Lycos, Inc., 478 F.3d 413 (1st Cir. 2007) (securities law); Zeran v. Am. Online, Inc., 129 F.3d 327 (4th Cir. 1997) (defamation); Doe v. MySpace, Inc., 474 F. Supp. 2d 843 (W.D. Tex. 2007) (child molestation by online predator); Chi. Lawyers' Comm. for Civil Rights Under the Law, Inc. v. Craigslist, Inc., 461 F. Supp. 2d 681 (N.D. Ill. 2006) (fair housing); Faegre & Benson, LLP, v. Purdy, 367 F. Supp. 2d 1238 (D. Minn. 2005) ("appropriation"); Blumenthal v. Drudge, 992 F. Supp. 44 (D.D.C. 1998) (defamation); Barrett v. Rosenthal, 146 P.3d 510 (Cal. 2006) (invasion of privacy); Gentry v. eBay, Inc., 121 Cal. Rptr. 2d 703 (Cal. Ct. App. 2002) (negligence); Doe v. Am. Online, Inc., 783 So. 2d 1010 (Fla. 2001) (child pornography); Schneider v. Amazon.com, Inc., 31 P.3d 37 (Wash. Ct. App. 2001) (breach of contract).

effort at rights clearance would debilitate the Internet.[3] Google has no realistic way of knowing which of the over 10 billion Web pages it searches might have information on it that violates the rights of someone else. If we forced Google to try to find out which Web pages have problematic materials on them, there is no way it could return automated search results. Even if it employed an army of lawyers to scrutinize all of the content, it would still be in no position to tell which pages were infringing or defamatory.[4] And even if it somehow figured out the answer for any given search result, it would have to determine the answer anew each time the search was run, because Web pages change frequently.

While the logic of some sort of safe harbor for Internet intermediaries is clear, the actual content of those safe harbors is not. Rather, the safe harbors actually in place are a confusing and illogical patchwork. For some claims, the safe harbors are absolute. For others, they preclude damages liability but not injunctive relief. For still others, they are dependent on the implementation of a "notice and takedown" system and a variety of other technical measures. And for at least a few types of claims, there may be no safe harbor at all. This patchwork makes no sense. In this article, I suggest that it be replaced with a uniform safe harbor rule. That suggestion is hopefully uncontroversial. The harder part is deciding what that uniform rule should be. I argue that the best model is the trademark immunity statute, one that lawyers and courts have so far almost completely ignored.

I. THE DIGITAL HOLE IN ISP SAFE HARBORS

The strongest safe harbor, and the one with the broadest applicability, arose largely by accident. In 1996, Congress passed the Communications Decency Act in an effort to make the Internet off limits to adult speech.[5] As part of that Act, Congress responded to concerns that Internet service providers ("ISPs") that took efforts to filter out objectionable content would render themselves liable for defamation as publishers by passing section 230 of the Act. That section provides:

> No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information

3. For a related argument – that search engines deserve special legal protection because they help society deal with information overload through automated sorting of content – *see* Frank Pasquale, *Copyright in an Era of Information Overload: Toward the Privileging of Categorizers*, 60 VAND. L. REV. 135 (2007).

4. I discuss objections to safe harbors, and group or automated responses an intermediary might adopt, below.

5. Communications Decency Act of 1996, Pub. L. No. 104-104, tit. V, 110 Stat. 133 (1996) (codified as amended in scattered sections of 47 U.S.C.).

> provided by another information content provider. . . . No cause of action may be brought and no liability may be imposed under any State or local law that is inconsistent with this section.[6]

The Communications Decency Act was quickly struck down as unconstitutional.[7] But section 230 survived. Indeed, it flourished. It has been interpreted quite broadly to apply to any form of Internet intermediary, including employers or other companies who are not in the business of providing Internet access[8] and even to individuals who post the content of another.[9] And it has been uniformly held to create absolute immunity from liability for anyone who is not the author of the disputed content,[10] even after they are made aware of the illegality of the posted material[11] and even if they fail or refuse to remove it.[12] The result is that Internet intermediaries need not worry about the legality of the content others post or send through their system, with one significant exception: section 230 does not apply to intellectual property ("IP") claims.[13]

The IP exemption from section 230 creates a gaping digital hole in Internet intermediary immunity. Two statutory provisions partially fill that gap. The first are the copyright safe harbors enacted in the Digital Millennium Copyright Act ("DMCA") in 1998.[14] Those safe harbors create immunity from monetary liability for copyright infringing material posted or sent through an intermediary's system. But they are subject to a number of requirements and limitations. First, unlike section 230, the DMCA safe harbors don't prevent suit for injunctive relief against an

---

6. 47 U.S.C. § 230(c)(1), (e)(3).

7. *See* Reno v. ACLU, 521 U.S. 844 (1997).

8. *See, e.g.*, Delfino v. Agilent Techs., Inc., 145 Cal. App. 4th 790, 804-08 (2006).

9. *See Barrett*, 146 P.3d at 513.

10. *See* cases cited *supra* note 2.

11. *Lycos*, 478 F.3d at 415.

12. *Zeran*, 129 F.3d at 328; Eckert v. Microsoft Corp., No. 06-11888, 2007 WL 496692, at *2-*4 (E.D. Mich. Feb. 13, 2007).

13. 47 U.S.C. § 230(e)(2); *Lycos*, 478 F.3d at 415 (refusing to apply section 230 to a state trademark dilution claim); Gucci Am., Inc. v. Hall & Assocs., 135 F. Supp. 2d 409, 412-14 (S.D.N.Y. 2001). There are other statutory exceptions as well. For example, violation of the Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848 (codified as amended in scattered sections of 18 U.S.C.), is exempt from section 230 immunity, as are violations of criminal statutes such as child pornography. *See* 47 U.S.C. § 230(c)(4). And a few courts have refused to apply section 230 in specialized circumstances. *See* Fair Hous. Council of San Fernando Valley v. Roommates.com, LLC, 489 F.3d 921 (9th Cir. 2007) (refusing to apply section 230 to housing discrimination claims by stretching to find that the intermediary was itself involved in publishing content); Avery v. Idleaire Techs. Corp., No. 3:04-CV-312, 2007 WL 1574269, at *20 (E.D. Tenn. May 20, 2007) (workplace harassment claim based on pornography downloaded on company computers).

14. 17 U.S.C. § 512.

intermediary.[15] Second, they don't protect all Internet intermediaries, but only four classes of intermediaries – conduit providers such as telephone companies,[16] those who store or cache content hosted by another,[17] those who host content posted by another,[18] and search engines.[19] Because those classes were fixed in the statute in 1998, their application to later-developed technologies such as peer-to-peer ("p2p") networks and online marketplaces has not always been clear.[20] Third, most of those protected intermediaries benefit from the safe harbor only if they establish, publicize, and implement both a notice and takedown system for removing all content about which copyright owners complain and a system for identifying "repeat infringers" and kicking them off the system,[21] and only if they accommodate technical protection measures.[22] Finally, the safe harbors for linking and content hosting sites contain a provision that may undo the benefits of the safe harbors altogether. It provides that the safe harbor is unavailable to any site that meets the then-existing legal standards for vicarious infringement.[23] The overall

---

15. *Id.* § 512(j).
16. *Id.* § 512(a).
17. *Id.* § 512(b).
18. *Id.* § 512(c).
19. *Id.* § 512(d).
20. *Compare* A&M Records, Inc. v. Napster, Inc., No. C 99-05183 MHP, 2000 WL 573136 (N.D. Cal. 2000) (rejecting section 512 immunity of a company that provided an indexing feature for infringing music supplied by others), *with* Hendrickson v. eBay, Inc., 165 F. Supp. 2d 1082 (C.D. Cal. 2001) (online auction site qualified for safe harbor as to listings of allegedly infringing copies of movies), *and* Corbis Corp. v. Amazon.com, Inc., 351 F. Supp. 2d 1090 (W.D. Wash. 2004) (online marketplace immune from liability for copyright infringement by its vendors).
21. 17 U.S.C. § 512(c)(2)-(3) (notice and takedown); § 512(i)(1)(A) ("repeat infringers").
22. *Id.* § 512(i)(1)(B).
23. *Id.* § 512(c)(1)(B) (safe harbor available only to an intermediary that "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"). The language suggests that it provides a safe harbor under section 512(c) only against claims of direct and contributory infringement, rather than vicarious liability. The legislative history suggests the opposite. *See* H.R. REP. No. 105-551, pt. 2, at 50 (1998) (suggesting – wrongly – that the bill would "protect qualifying service providers from liability for all monetary relief for direct, vicarious, and contributory infringement"). And the fact that the statute doesn't use the term vicarious infringement, but instead sets out what were commonly understood in 1998 to be the elements of a vicarious infringement claim, raises additional questions. The Ninth Circuit has steadily whittled away the requirement of "direct financial benefit" as a requirement for vicarious infringement, for instance, to the point where it has held parties liable in the absence of any financial benefit at all, direct or indirect. *See* A&M Records, Inc. v. Napster, Inc., 239 F.3d 1004 (9th Cir. 2001); *cf.* Fonovisa, Inc. v. Cherry Auction, Inc., 76 F.3d 259 (9th Cir. 1996) (beginning the whittling away of the "direct financial benefit" requirement completed in *Napster*). And the Supreme Court has created a new tort for inducement of copyright infringement, though it claimed that this new tort was an offshoot of contributory infringement. Metro-Goldwyn-Mayer Studios Inc. v. Grokster, Ltd., 545 U.S. 913 (2005). Are these new or broadened torts also outside the safe harbor? A plain reading of the statute would suggest not, but to date there is no case law on the issue.

effect is a set of "safe harbors" that provides something less than perfect safety for intermediaries, and that gives intermediaries incentives to take down any doubtful content as soon as they receive a complaint about it.

Less well-known than the copyright safe harbors is section 32(2) of the Lanham Act,[24] which creates a form of safe harbor from trademark infringement for publishers and extends the definition of publishers to online providers of content written by another.[25] The relevant portions of the statute provide:

> **(B)** Where the infringement or violation complained of is contained in or is part of paid advertising matter in a newspaper, magazine, or other similar periodical or in an electronic communication as defined in section 2510(12) of Title 18, the remedies of the owner of the right infringed or person bringing the action under section 1125(a) of this title as against the publisher or distributor of such newspaper, magazine, or other similar periodical or electronic communication shall be limited to an injunction against the presentation of such advertising matter in future issues of such newspapers, magazines, or other similar periodicals or in future transmissions of such electronic communications. The limitations of this subparagraph shall apply only to innocent infringers and innocent violators.
>
> **(C)** Injunctive relief shall not be available to the owner of the right infringed or person bringing the action under section 1125(a) of this title with respect to an issue of a newspaper, magazine, or other similar periodical or an electronic communication containing infringing matter or violating matter where restraining the dissemination of such infringing matter or violating matter in any particular issue of such periodical or in an electronic communication would delay the delivery of such issue or transmission of such electronic communication after the regular time for such delivery or transmission, and such delay would be due to the method by which publication and distribution of such periodical or transmission of such electronic communication is customarily conducted in accordance with sound business practice, and not due to any method or device adopted to evade this section or to prevent or delay the issuance of an injunction or restraining order with respect to such infringing matter or violating matter.[26]

---

24. 15 U.S.C. § 1114(2).

25. *Id.* § 1114(2)(B)-(C).

26. *Id.* While this exclusion applies only to trademark infringement and unfair competition, and not to trademark dilution, a safe harbor for ISPs from the dilution statute is unnecessary because that statute itself provides that they are not liable at all for dilution:

> The following shall not be actionable as dilution by blurring or dilution by tarnishment under this subsection:

This exemption has only rarely been applied by the courts, and seems to be unknown even to many trademark lawyers.[27] It exempts at least some Internet intermediaries – those who are "innocent infringers," a term that is not defined in the Lanham Act – from damages liability, and also from liability for injunctive relief in circumstances where an injunction would interfere with the normal operation of the online publisher. In *Hendrickson v. eBay*, the only case applying this section to the Internet, the court read it to confer broad immunity:

> Plaintiff seeks an injunction enjoining any and all false and/or misleading advertisements that may be posted on eBay's website by users in the future, regardless of whether they are the basis of this lawsuit and whether they have been identified by Plaintiff.
>
> No authority supports Plaintiff's position. Indeed, such an injunction would effectively require eBay to monitor the millions of new advertisements posted on its website each day and determine, on its own, which of those advertisements infringe Plaintiff's Lanham Act rights. As the Court previously noted, "no law currently imposes an affirmative duty on companies such as eBay to engage in such monitoring." . . . eBay has no affirmative duty to monitor its own website for potential trade dress violation and Plaintiff had failed to put eBay on notice that particular advertisements violated his Lanham Act rights before filing suit.[28]

But it is not clear how broadly the exemption applies to Internet intermediaries like backbone providers who are not themselves publishing the content including the trademark. Perhaps they don't need an exemption because they are not engaged in trademark use,[29] but the

---

> (A) Any fair use, including a nominative or descriptive fair use, or facilitation of such fair use, of a famous mark by another person other than as a designation of source for the person's own goods or services, including use in connection with—
> (i) advertising or promotion that permits consumers to compare goods or services; or
> (ii) identifying and parodying, criticizing, or commenting upon the famous mark owner or the goods or services of the famous mark owner.
> (B) All forms of news reporting and news commentary.
> (C) Any noncommercial use of a mark.

15 U.S.C. § 1125(c)(3). While this language is not a model of clarity, both the reference to use "other than as a designation of source" and to "facilitation" of uses by others would seem to protect ISPs who merely make available the content of others. *Id.*

27. A panel devoted to third-party liability for trademark infringement online at the International Trademark Association meeting did not discuss the section at all, for example.

28. *Hendrickson*, 165 F. Supp. 2d at 1095 (citation omitted).

29. *See, e.g.*, Stacey L. Dogan & Mark A. Lemley, *Grounding Trademark Law Through Trademark Use,* 92 IOWA L. REV. 1669 (2007) [hereinafter Dogan & Lemley, *Grounding*]; Stacey L. Dogan & Mark A. Lemley, *Trademarks and Consumer Search Costs on the Internet*,

applicability of the trademark use requirement has been controversial[30] and it is possible that a variety of Internet intermediaries could be sued for direct trademark infringement.

Finally, there is no explicit statutory safe harbor for hosting, transmission, or linking to content that is alleged to violate other types of IP. Internet intermediaries face liability for infringement of patents even if they did not themselves post or authorize the content that turns out to infringe the right. The same may also be true of state IP rights such as the right of publicity and misappropriation of trade secrets, though there is a conflict in the circuits over whether section 230 immunity extends to such state IP rights.[31] It may even be true of violations of the anti-circumvention provisions of the DMCA, if those provisions are read to create secondary liability against those who host or link to anti-circumvention tools.[32] And while the intermediary may have no knowledge of the infringement, that will not protect them from charges of patent or right of publicity infringement because both are strict liability offenses.[33] Nor will it protect them from the occasional claim for direct infringement of other IP rights.[34]

II. STANDARDIZING SAFE HARBORS

A. The Need for Standardization

The patchwork of safe harbors is a result of accident, not design.

---

41 HOUS. L. REV. 777 (2004).

30. *Compare* Graeme B. Dinwoodie & Mark D. Janis, *Confusion Over Use: Contextualism in Trademark Law*, 92 IOWA L. REV. 1597 (2007) (arguing for abolition of the trademark use doctrine), *with* Dogan & Lemley, *Grounding*, *supra* note 29 (defending the doctrine).

31. *Compare Lycos*, 478 F.3d at 418 (assuming that section 230 did not immunize an ISP from liability under a state trademark dilution statute), *with* Perfect10, Inc. v. CCBill LLC, 488 F.3d 1102, 1118-19 (9th Cir. 2007) (holding that "intellectual property" in the exclusion from section 230 immunity means only federal IP rights, not the right of publicity).

32. Whether there is any such theory of secondary DMCA liability is unclear. The DMCA is itself a secondary liability statute, and I am skeptical that tertiary liability – facilitating others whose offense is facilitating still others to infringe copyrights – is or should be a part of the DMCA scheme. But the issue is not free from doubt. *Cf.* Gordon v. Nextel Commc'ns, 345 F.3d 922, 925-27 (6th Cir. 2003) (approving a vicarious liability theory under 17 U.S.C. § 1202 in dealing with alteration of copyright management information).

33. Fla. Prepaid Postsecondary Educ. Expense Bd. v. Coll. Sav. Bank, 527 U.S. 627, 646 (1999) (holding patent infringement does not require proof of intent to infringe); 1 J. THOMAS MCCARTHY, THE RIGHTS OF PUBLICITY AND PRIVACY § 3:27 (2d ed. 2004). Trade secret misappropriation, however, likely requires at least negligence as to the secret status of the information, *see, e.g.*, Cal. Civ. Code § 3426.1(b) (West 2007) (requiring that the defendant knows or has reason to know it is stealing a trade secret), so the risk of liability is lessened there.

34. *See, e.g.*, Complaint at 2-5, Stovall v. Yahoo! Inc., No. 1:07-Civ-00573 (N.D. Ohio Feb. 27, 2007).

The safe harbors arose haphazardly and not always even intentionally. The lack of standardization is problematic for several reasons. First, the absence of any safe harbor for IP infringement other than copyright and trademark (at least outside the Ninth Circuit) creates a hole in the safe harbors, exposing Internet intermediaries to risk of liability and potentially causing them to respond differently to such claims. Second, unsophisticated intermediaries may not be aware of the many nuances in the safe harbors, and may wrongly think they can rely on a safe harbor that does not in fact apply to their circumstance. As a result, they may not react efficiently to charges of infringement. Indeed, I am aware of a number of intermediaries that treat any content-based complaints they receive under the DMCA, whether or not those complaints involve copyrights. Even more likely, unsophisticated plaintiffs and their lawyers may not understand the differences between the safe harbor rules, and therefore file lawsuits that have no chance of success (or decide to forego suits that could in fact be meritorious).

A third problem is the uncertain scope of the IP exception in section 230. We can be quite confident that it applies to patents, copyrights, and trademarks, somewhat less confident that trade secrets and the right of publicity are also IP claims,[35] and even less confident for the penumbra of quasi-IP claims. Cases in this latter category area include the doctrines of misappropriation,[36] idea submission, and state moral rights claims.[37] If all these claims are in fact IP claims, as the First Circuit has assumed,[38] section 230 does not apply and there is no safe harbor at all. If, on the other hand, they are merely state tort claims, as the Ninth Circuit has held with respect to the right of publicity,[39] the absolute immunity of section 230 protects intermediaries.

The inconsistent treatment of different types of claims also leads to litigation abuses by plaintiffs who seek to recast claims subject to significant immunity as different types of claims with lesser or nonexistent immunity. I will give just two examples. First, FedEx threatened an individual who made furniture for his home out of FedEx boxes and put up a Web page at fedexfurniture.com showing pictures of

---

35. *See* Stacey L. Dogan & Mark A. Lemley, *What the Right of Publicity Can Learn From Trademark Law*, 58 STAN. L. REV. 1161, 1163-68 (2006) (describing the history of the right of publicity as a privacy tort rather than an IP right); *cf.* Robert G. Bone, *A New Look at Trade Secret Law: Doctrine in Search of Justification*, 86 CAL. L. REV. 241 (1998) (challenging the fit of trade secrets within the IP framework).

36. *Cf. Faegre & Benson*, 367 F. Supp. 2d at 1248 (preempting appropriation claim that sounded in IP).

37. *See Perfect10*, 488 F.3d at 1118 ("[S]tate laws protecting 'intellectual property,' however defined, are by no means uniform. Such laws may bear various names, provide for varying causes of action and remedies, and have varying purposes and policy goals.").

38. *Lycos*, 478 F.3d at 415.

39. *Perfect10*, 488 F.3d at 1121.

the furniture and how to build it. To the (doubtful) extent that FedEx had any claim at all, it was a trademark claim based on the use of the domain name. But if FedEx asserted only trademark claims, it could not coerce an ISP into taking down the Web site, so it asserted a (entirely bogus) copyright claim instead.[40] Similarly, the husband of a baron in Second Life whose avatar was the subject of an offensive video sent a DMCA copyright notice to YouTube in an effort to have the video removed.[41] The plaintiff might have had a defamation or invasion of privacy claim, but YouTube would have been entirely immune from liability for those claims under section 230. By mischaracterizing tort claims as copyright claims, plaintiffs seek to take advantage of a more favorable legal regime. This sort of gamesmanship is undesirable.

The inconsistencies in the current safe harbors may affect ISP behavior in undesirable ways as well. The stated purpose of section 230 was to give ISPs the freedom to exercise editorial control over content on their sites without being deemed a "publisher" subject to liability for the content choices it makes. But because copyright law has a different rule, exercising that editorial control can be evidence leading to a finding of vicarious liability in a copyright case. As a result, ISPs may be unwilling to establish or exercise any power to excise harmful content from the site even in a tort case covered by section 230, lest doing so take them outside the copyright safe harbor.

Against these arguments for standardization, some might claim that the differential treatment of safe harbors is desirable. Copyright owners, for instance, might allege that copyright infringement is a worse problem than online defamation, and that they should therefore have more power to reach third parties involved somehow in that infringement. But the patchwork of current rules is unlikely to correspond to good policy in particular cases except by accident. Perhaps there is an argument that as a matter of policy there should be complete immunity from right of publicity claims, strong immunity from trademark claims, weaker and conditional immunity for copyright claims, and no immunity from patent claims, but I'm skeptical. More likely, people who benefit from particular rules – ISPs and anonymous defendants in the case of section 230, copyright owners in the case of the DMCA – have come to view those rules as entitlements and to object to anything that changes the status quo. But the fact that we've done it this way for ten years[42] is not

40. *See* Wikipedia, Fed Ex Furniture, http://en.wikipedia.org/wiki/FedEx_furniture (last visited Sept. 17, 2007).

41. *See* Daniel Terdiman, *DMCA Complaint Against YouTube Dropped*, ZDNET NEWS, Jan. 15, 2007, http://news.zdnet.com/2100-9588_22-6150216.html?part=rss&tag=feed&subj=zdnn.

42. It may even be less than ten years. The DMCA was adopted in 1998, but applications of those safe harbors to new technologies came later. And some of the rules are still unclear,

a strong argument that it must always be done this way. In the next section, I discuss some of the problems with particular rules. In the absence of some reason to treat different causes of action differently, there are a variety of benefits to standardization.

B. Standardization on What?

If we are to replace the patchwork of safe harbors in the existing law with a uniform rule covering both IP and other tort claims, what should that rule look like? There are four basic possibilities: no safe harbor at all, complete immunity, a notice and takedown regime modeled on the DMCA, or a no-damages, no-interference regime modeled on the trademark statute. I consider each in turn.

1. No safe harbor

A few scholars have argued for liability for Internet intermediaries, contending that imposing liability on those intermediaries will give them efficient incentives to identify and block infringing or other offensive material.[43] Whatever the abstract merits of this cost-internalization rationale in theory, in practice, I think it is likely to be a disaster. It is simply impossible for a search engine – to say nothing of an ISP or bandwidth conduit – to cull through the literally billions of links and messages they process every day and identify all those messages and Web pages that may create liability under any law. This is not just a technical problem of assessing those petabytes of data, though comparing everything on the Web to everything ever copyrighted in real time is computationally infeasible with existing or any foreseeable technology. Rather, the deeper problem is that there is no way to automate the process of determining legal liability. Software can perhaps strip certain offensive words out of email text, though even the offensiveness of words turns out to be surprisingly contextual, as those who have dealt with Web filtering software have discovered. But there is no way for them to determine whether a message defames another, or violates the securities laws, or invades the privacy of another, or constitutes a trademark use likely to confuse consumers. Image-parsing software may someday be able to identify pictures or videos that are similar to

---

as the *Viacom v. Google* case demonstrates. *See* Complaint, Viacom Int'l Inc. v. YouTube, Inc., No. 1:2007-CV-02103 (S.D.N.Y. Mar. 13, 2007).

43. Douglas Lichtman & William Landes, *Indirect Liability for Copyright Infringement: An Economic Perspective*, 16 HARV. J.L. & TECH. 395 (2003); *see also* Susan Freiwald, *Comparative Institutional Analysis in Cyberspace: The Case of Intermediary Liability for Defamation*, 14 HARV. J.L. & TECH. 569 (2001). *Cf.* Doug Lichtman & Eric Posner, *Holding Internet Service Providers Accountable*, 14 SUP. CT. ECON. REV. 221 (2006) (making a case for ISP liability for viruses and software flaws, but distinguishing copyright infringement).

individual copyrighted works, but they will never be able to determine whether those pictures are fair uses, or whether they are legitimate copies or displays made under one of the many statutory exceptions, or whether the individual pictured is 16 rather than 18 years of age. Add to all of this the fact that it is not just every law in the U.S. but the overlapping, sometimes-inconsistent legal rules of every country that intermediaries would have to apply, and you begin to see the scope of the problem.

Lichtman and Landes acknowledge this problem, but reply that Internet intermediaries don't need to weed out this infringing material; they can simply compensate the universe of all plaintiffs for harm suffered as a result of the Internet, and pass the cost of that compensation on to their users.[44] But that won't work either. To begin, it is worth noting that capping ISP liability at cost internalization is not even possible under the current copyright regime because the Copyright Act provides for a floor of statutory damages ($750 per work) that will often exceed by orders of magnitude the harm actually suffered by copyright owners. If YouTube, eBay, Yahoo!, Verizon, Comcast, and others face the prospect of tens of billions of dollars in statutory damages for hosting, carrying, or linking to content whose provenance they cannot determine, they will either go out of business or they will impose restrictions on the content they will carry sufficiently onerous that they would effectively lock down the Internet. A similar problem results from the fact that the IP rules in particular are commonly protected by property rules. A court that enjoins the display of infringing material may effectively end up enjoining the operation of the Internet intermediary altogether because there is no way for the intermediary to block the infringing material from every source without blocking lots of non-infringing material as well.[45] At a minimum, therefore, treating ISPs as cost aggregators would require elimination of statutory damages rules, punitive damages in tort, and all injunctive relief.

But even as to laws that do limit remedies to compensatory damages – defamation, say – passing liability on to Internet intermediaries will not result in efficiency. Because there is no obvious way for search engines, ISPs, or conduit providers to distinguish infringing from non-infringing content ex ante, those intermediaries cannot simply refuse to deal with infringers. Rather, they will have to serve as "Internet insurers," spreading the risk of all types of harm to all their members. This would create what is arguably the largest moral hazard problem ever seen. If you are paying your ISP thousands of dollars for connectivity because millions of people are using the Internet to trade music for free, you

44. Lichtman & Landes, *supra* note 43, at 404-07.

45. Mark A. Lemley & Philip J. Weiser, *Should Property or Liability Rules Govern Information?*, 85 TEX. L. REV. 783 (2007).

would be a fool not to download your music illegally. Replacing a regime under which tortfeasors are liable with one under which technology companies are liable and tortfeasors can act with impunity seems unlikely to efficiently control tortious behavior.

Finally, there is an even more systematic problem with treating Internet intermediaries as cost-bearers. Intermediaries do not and cannot reasonably expect to capture anything like the full social value of the uses that pass through their system. If we impose the full social costs of harm from third party postings on intermediaries, but they cannot capture the full social benefits of those postings, they will respond by inefficiently restricting the uses that third parties can make of the Internet.[46] Given that Internet access is not the sort of conduct in which the externalized harms significantly exceed the externalized benefits, a strict liability approach of this sort is likely to be inefficient.[47] If we adopt it, the only intermediaries we see are ones that, like cable networks, transmit only pre-approved content from a short list of providers. The amazing diversity of the Internet, with its abundance of user-generated content, would be impossible.

2. Absolute safe harbor

At the opposite end of the safe harbor spectrum is section 230. While that section was arguably intended only to have the limited effect of overruling a few decisions that had treated ISPs as speakers for defamation purposes,[48] courts interpreting it have unanimously read it more broadly, as creating absolute immunity for ISPs and anyone else who is not the author of the content for which liability is asserted. Applying absolute immunity to IP claims as well would certainly solve the liability and moral hazard problems described above. And some will argue that section 230 has worked well for non-IP torts, and so could be expanded to IP cases as well without fear of harm. But I think this approach goes too far in the other direction. Under section 230 today,

---

46. For an economic demonstration of this point, *see* Brett M. Frischmann & Mark A. Lemley, *Spillovers*, 107 COLUM. L. REV. 257 (2007).

47. For a detailed economic analysis along these lines, with particular attention to cybersecurity issues, *see* Keith N. Hylton, *Property Rules, Liability Rules, and Immunity: An Application to Cyberspace*, 87 B.U. L. REV. 1 (2007).

48. *See* H.R. REP. No. 104-458, at 194 (1996) (Conf. Rep.). The particular case that triggered Congressional concern was Stratton Oakmont, Inc. v. Prodigy Servs. Co., No. 031063/94, 1995 WL 323710 (N.Y. Sup. Ct. May 24, 1995), which had held Prodigy strictly liable for republishing a defamatory statement; *see also* Cubby, Inc. v. CompuServe, Inc., 776 F. Supp. 135 (S.D.N.Y. 1991) (recognizing a distinction between those who affirmatively publish a libel and those who merely distribute it, and treating ISP as a distributor subject to lesser liability). For a discussion of the legislative history, *see* Ken S. Myers, *Wikimmunity: Fitting the Communications Decency Act to Wikipedia*, 20 HARV. J.L. & TECH. 163, 174-78 (2006).

ISPs have no incentive to police their sites even for content that obviously does not belong there, or to take down even material that is clearly false or injurious. Nor are they even obligated to aid the plaintiff in finding the wrongdoer by disclosing the identity of their clients.[49] As a result, absolute immunity may lead to plaintiffs being unable to remove objectionable material or to find the tortfeasor in order to recover damages from her, and therefore remaining uncompensated even for egregious harms. Expanding this absolute safe harbor to IP cases would be particularly problematic if copyright owners had no way to find the people who were actually cracking their encryption systems and posting their content online.

3. Notice and takedown

The copyright safe harbors built into the DMCA solve these problems by conditioning immunity from liability on an ISP or other intermediary (1) taking down material once the copyright owner has complained of it,[50] (2) identifying its customers once it receives a subpoena,[51] and (3) terminating repeat infringers.[52] The DMCA therefore represents a sort of middle ground between the extremes of no liability and unrestricted liability.

Nonetheless, the DMCA safe harbors have a number of problems. First, they were drafted in 1998 to carve out specific intermediaries, rather than creating a general protection for Internet intermediaries hosting, passing through, or linking to the content of another. As a result, they almost immediately became obsolete as new technologies – most notably p2p networking – were developed. As new business models develop, and as companies in the existing categories change the way they work, the specific categories of the DMCA are likely to be less and less relevant. Thus, a potential advantage of the DMCA approach – the fact that it treats different types of intermediaries differently – has become, over time, a problem instead.

Second, the safe harbor for content hosting companies in section

49. In *Zeran v. America Online*, for example, an anonymous poster offered T-shirts making fun of the Oklahoma City terrorist bombing less than a week after it occurred, and said the T-shirts were available at Zeran's phone number. *Zeran*, 129 F.3d at 329. As a result, Zeran received a constant stream of abusive calls and death threats. *Id.* AOL eventually removed the postings, but never identified the perpetrator. *Id.*

50. 17 U.S.C. § 512(c)(1)(C).

51. *Id.* § 512(h).

52. *Id.* § 512(i)(1)(A). As David Nimmer has pointed out, however, it is not at all clear what it means to be a repeat infringer. David Nimmer, *Repeat Infringers*, 52 J. COPYRIGHT SOC'Y 167 (2005). *Cf.* Mark A. Lemley & R. Anthony Reese, *A Quick and Inexpensive System for Resolving Peer-to-Peer Copyright Disputes*, 23 CARDOZO ARTS & ENT. L.J. 1 (2005) (offering a middle ground on the issue).

512(c) contains what may turn out to be a gaping loophole – it does not protect any intermediary who is engaged in conduct that the law at that time defined as vicarious infringement.[53] Courts have been expanding the scope of vicarious infringement over time, concluding that "direct financial benefit" required for vicarious infringement could be satisfied without proof of any revenue at all,[54] and that the "ability to control" infringement was satisfied if a landlord or site owner could stop infringement by shutting down the whole system.[55] They have also created an entirely new doctrine of copyright infringement inducement whose status within the indirect liability framework is unclear.[56] A "safe harbor" that opens ISPs to liability whenever a plaintiff can allege that the ISP is making money in part from customer infringement and that it could do more than it does to prevent infringement is a weak shelter indeed.[57]

Finally, the effect of the notice and takedown system has been to encourage Internet intermediaries to take down any and all content copyright owners complain of, no matter how frivolous the complaint.[58] Indeed, a recent study of DMCA takedowns found that 30% of them were legally dubious at best.[59] While the law is even-handed and provides for a mechanism for posters to get their content put back,[60]

---

53. 17 U.S.C. § 512(c)(1)(B) (safe harbor available only to an intermediary that "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").

54. *A&M Records*, 239 F.3d at 1004.

55. *Id.*; *Fonovisa*, 76 F.3d at 259.

56. *Grokster*, 545 U.S. at 913.

57. Section 512(c) contains other loopholes as well, including one limiting immunity to intermediaries that are "not aware of facts or circumstances from which infringing activity is apparent." 17 U.S.C. § 512(c)(1)(A)(ii). While it seems reasonably clear that this sort of "red flag" knowledge is intended to apply only to require intermediaries to remove specific content they discover and strongly suspect is infringing – were that not so, this provision would swallow the entire safe harbor – uncertainty about its meaning has allowed Viacom to bring a copyright lawsuit against YouTube and allege that YouTube does not qualify for the safe harbor, despite YouTube's compliance with over 100,000 Viacom DMCA takedown notices. *See* Geraldine Fabrikant & Saul Hansell, *Viacom Tells YouTube: Hands Off*, N.Y. TIMES, Feb. 3, 2007, at C1.

58. On this problem, *see, e.g.*, Assaf Hamdani, *Who's Liable for Cyberwrongs?*, 87 CORNELL L. REV. 901 (2002); Neal Kumar Katyal, *Criminal Law in Cyberspace*, 149 U. PA. L. REV. 1003, 1007-08 (2001). Fred Yen argues that this tendency is exacerbated by the risk of enterprise liability faced by any ISP that doesn't fit within the safe harbors. Alfred C. Yen, *Internet Service Provider Liability for Subscriber Copyright Infringement, Enterprise Liability, and the First Amendment*, 88 GEO. L.J. 1833 (2000). *See generally* Seth F. Kreimer, *Censorship By Proxy: The First Amendment, Internet Intermediaries, and the Problem of the Weakest Link*, 155 U. PA. L. REV. 11, 11 (2006) (referring to efforts to "enlist Internet intermediaries as proxy censors").

59. *See* Jennifer M. Urban & Laura Quilter, *Efficient Process or "Chilling Effects"? Takedown Notices Under Section 512 of the Digital Millennium Copyright Act*, 22 SANTA CLARA COMPUTER & HIGH TECH. L.J. 621 (2006).

60. 17 U.S.C. § 512(g). Significantly, however, only hosting companies have to give

many posters are legally unsophisticated and don't know that they have this right or how to exercise it. Indeed, Urban and Quilter find that very few people avail themselves of this mechanism.[61] Notice and takedown therefore rewards overzealous copyright owners who use the DMCA mechanism to rid the Web even of legitimate content, secure in the expectation that ISPs will take everything down rather than risk their eligibility for the safe harbor.[62] This is a problem in copyright cases, but it's likely to be an even greater problem if a notice and takedown regime is extended to a variety of non-IP tort claims, including such First Amendment-sensitive issues as defamation and invasion of privacy. The notice and takedown approach has been applied outside IP in much of the rest of the world, and the consequences for speech have not been pretty.[63]

4. The trademark regime

An ideal safe harbor would take the middle ground approach of the DMCA, but would avoid some of its pitfalls. It would be general rather than specific in its application to Internet intermediaries. It would give plaintiffs the information they needed to find tortfeasors, and would give them a mechanism for quickly and cheaply removing objectionable content from the Web, but it would also discourage intermediaries from automatically siding with the plaintiff, and would give them real immunity against the specter of damages liability.

I think the trademark immunity statute comes the closest to an ideal approach. It is general in its scope, applying to offline as well as online publishers of content provided by another. It provides a complete immunity from damages liability for intermediaries that are "innocent infringers," and also prevents courts from granting overbroad injunctions that would hamper the operation of the intermediary in an effort to stop one particular act of infringement. It is not conditioned on a regime of automatic takedown, but at the same time it allows plaintiffs to get an

---

their customers notice before taking material down; search engines and caching sites do not.

61. Urban & Quilter, *supra* note 59, at 679-80. They find that fewer than 1% of all takedowns ever receive a putback notice, but that number may be artificially small because so many of the notices in their study were sent to search engines, which have no statutory obligation to notify a site when a search result is removed. *Id.* Even excluding all section 512(d) notices from their study, however, raises the number of putbacks to only 6%. *Id.*

62. There is a provision punishing anyone who "knowingly materially misrepresents" the copyright status of a work in a DMCA notice by subjecting them to liability for attorney's fees. 17 U.S.C. § 512(f). But it has been read narrowly, to exempt even those who have an objectively unreasonable belief in their case. *See* Rossi v. Motion Picture Ass'n of Am. Inc., 391 F.3d 1000, 1004-05 (9th Cir. 2004). As a result, only one case has actually awarded fees under section 512(f). Online Policy Group v. Diebold, Inc., 337 F. Supp. 2d 1195 (N.D. Cal. 2004). *Cf.* Marvel Enters., Inc. v. NCSoft Corp., No. CV-04-9253RGKPLAX, 2005 WL 878090 (C.D. Cal. Mar. 9, 2005) (refusing to dismiss a claim for fees).

63. For a brief discussion, see *infra* notes 73-78 and accompanying text.

injunction removing offensive content.

The trademark model is not perfect, however. Because litigation to an injunction would be costly, it may be that ISPs will still have an incentive to take down content in the face of a threat of suit, so the possibility of overbroad takedowns still exists in the trademark model. And without the notice and putback provisions in the DMCA, that incentive could exacerbate the overdeterrence problem already evident in copyright cases. The solution may be to borrow from another aspect of trademark law – the development of the Uniform Dispute Resolution Process ("UDRP") for resolving cybersquatting complaints. Tony Reese and I have elsewhere proposed a fast, cheap online arbitration for digital copyright disputes,[64] and something along those lines could be expanded to apply to claims made against ISPs for other types of content as well. The law should also include punishments for abuse of the takedown process.[65]

My only other concern with the trademark model is the vagueness of the term "innocent infringers." Were a court to interpret this language to preclude reliance on the safe harbor by anyone who had ever received a trademark complaint, it would undo the benefits of the safe harbor.[66] The legislative history makes it clear that this term is intended instead to invoke the rather strict standard of actual malice from the defamation cases:

> the revision sets forth critical constitutional protections that underlie changes made in section 43(a). It exempts from liability "innocent" disseminators of offending material, whether that material constitutes a violation of section 32(1), relating to infringement, or of proposed Section 43(a), relating to false and misleading commercial advertising. Most prominently, the change protects newspapers, magazines, broadcasters, and other media from liability for the innocent dissemination of commercial false advertising, including promotional material. The word "innocent" is intended to encompass the constitutional standards set forth in New York Times v. Sullivan, 376 U.S. 254 (1964) and its progeny.[67]

Assuming courts apply this standard, as at least one has done,[68] the safe

---

64. Lemley & Reese, *supra* note 52, at 1.

65. The DMCA has such a provision. 17 U.S.C. § 512(f).

66. In *Hendrickson v. eBay, Inc.*, the court did not face this issue, because there was no evidence that the defendant was even aware of the trademark claims before the suit was filed. *Hendrickson*, 165 F. Supp. 2d at 1095.

67. 134 CONG. REC. H31851 (daily ed. Oct. 19, 1988) (statement of Rep. Kastenmeier).

68. NBA Props. v. Untertainment Records LLC, No. 99 CIV 2933(HB), 1999 WL 335147, at *14 (S.D.N.Y. May 26, 1999) ("Adopting that view of the 'innocent' standard, the NBAP would have to prove that Vibe acted either (i) with knowledge that the publication infringed the NBAP's rights, or (ii) with reckless disregard as to whether the Advertisement

harbor should provide effective protection.

One other thing I think needs to be added to the trademark regime is a streamlined subpoena rule along the lines of what the DMCA attempted for copyright law.[69] If plaintiffs are unable to recover damages from Internet intermediaries, it seems only reasonable that they have recourse against the people actually causing the harm. The alternative – requiring a *Doe* lawsuit filed in a random court that may or may not (probably not) have jurisdiction over the defendant – has the advantage that the plaintiff can be forced to demonstrate the strength of its case before discovering the identity of the defendant.[70] But it has the disadvantages that it requires a lawsuit be filed when in many cases the issue could otherwise be resolved without litigation, and that it requires that lawsuit be filed when the plaintiff has no idea where the defendant resides, with the result that the parties are far more likely to engage in unnecessary litigation over personal jurisdiction.[71] An optimal procedure might steer a middle ground, allowing subpoenas upon a showing of good cause even without filing a lawsuit, but requiring the ISP to notify the defendant and give them a chance to anonymously contest the subpoena, either in court or in the sort of online administrative procedure I outlined above.

It is true that requiring intermediaries to retain and disclose the identity of their customers in response to a subpoena will make truly anonymous posting difficult (or even impossible, if no ISP is willing to forego the safe harbor in order to provide its customers with anonymous Internet access).[72] But that price may be worth paying for a system that

---

infringed NBAP's rights.").

69. The actual efficacy of the DMCA subpoena system was significantly weakened by the decisions in In re Charter Commc'ns, Inc., Subpoena Enforcement Matter, 393 F.3d 771 (8th Cir. 2005), and Recording Indus. Ass'n of Am., Inc. v. Verizon Internet Servs., Inc., 351 F.3d 1229 (D.C. Cir. 2003). In the wake of those decisions, copyright owners have had to file *Doe* lawsuits against unknown file sharers, and courts have not been receptive to grouping Does together, making it virtually impossible to pick a court that has jurisdiction over the unknown defendant. For a rare example of a suit against a file sharer that actually went to judgment, *see* BMG Music v. Gonzalez, 430 F.3d 888 (7th Cir. 2005). Congress's goal was to create a streamlined procedure that did not require lawsuits filed against unknown parties, and that goal seems a reasonable one. But after the decisions in *Charter* and *Verizon* it will take legislative change to implement such a procedure.

70. For examples of this procedure under current tort law, *see, e.g.*, Doe v. 2TheMart.com Inc., 140 F. Supp. 2d 1088 (W.D. Wash. 2001); In re Subpoena Duces Tecum to Am. Online, Inc., No. 40570, 2000 WL 1210372 (Va. Cir. Ct. Jan.31, 2000), *rev'd*, 542 S.E.2d 377 (2001).

71. In some cases, circumstances may suggest that the defendant resides within the jurisdiction. For example, subpoenas to universities are likely to find defendants who reside at or near the university.

72. Under my approach, ISPs who wish to qualify for the safe harbor must keep records of who has posted the material. Other ISPs could opt to provide anonymity to consumers who desire it, as Freenet and Earthstation 5 already do. *See* John Alan Farmer, Note, *The Specter of*

allows redress of real harms without overwhelming ISPs with liability. It is worth noting in this regard that most people who think they have anonymity now do not in fact have it, and that the existing DMCA system effectively requires ISPs to disclose the identity of their customers in copyright cases, a rule that has not led to widespread problems as far as I can tell.

C. International Standardization

Changing U.S. law to standardize on a safe harbor will solve only part of the problem facing Internet intermediaries. Other countries, particularly in Europe, have not yet fully understood the benefit of insulating Internet intermediaries from unreasonable liability, perhaps because the intermediary defendants have largely been American companies and the plaintiffs have all been local. While the EC's 2000 Electronic Commerce Directive[73] provides for some safe harbors, they do not appear to be working, at least as implemented in national legislation and the courts.[74] Those courts have regularly found intermediaries liable for selling Nazi memorabilia,[75] linking to sites containing copyrighted material,[76] or allowing competitors to run advertisements opposite search results.[77] And Europe in particular is contemplating going even further,

---

Crypto-Anarchy: Regulating Anonymity-Protecting Peer-to-Peer Networks, 72 FORDHAM L. REV. 725, 726 (2003) (pointing to Freenet as a means for circumventing legal regulation). But the law may render any hope of anonymity on the part of ISP consumers irrelevant; pending federal legislation would require ISPs to keep records of postings so the government could access it. Declan McCullagh, *GOP Revives ISP-tracking Legislation*, CNET NEWS.COM, Feb. 6, 2007, http://news.com.com/2100-1028_3-6156948.html. That legislation would presumably trump the state constitutional right to privacy of ISP data that some courts have recognized. *See* State v. Reid, 914 A.2d 310 (N.J. Sup. Ct. App. Div. 2007). Similar legislation is already in force in other countries. *See, e.g.*, Council Directive 2006/24/EC, Retention of Data Generated or Processed in Connection with the Provision of Publicly Available Electronic Communication Services, 2006 O.J. (L105).

73. For a discussion, *see* Rosa Julia-Barcelo, *On-line Intermediary Liability Issues: Comparing E.U. and U.S. Legal Frameworks*, 22 EUR. INTELL. PROP. REV. 105 (2000).

74. Part of the problem is that the Directive seems to contemplate ISP liability for negligence in allowing infringing material to be posted. Council Directive 2000/31/EC, art. 14, 2000 O.J. (L178). *See also* Gerald Spindler & Matthias Leistner, *Secondary Copyright Infringement – New Perspectives in Germany and Europe*, 37 INT'L REV. INTELL. PROP. & COMPETITION L. 788, 789 (2006).

75. *See* Yahoo! Inc. v. La Ligue Contre la Racisme et L'Antisemitisme, 433 F.3d 1199, 1201-05 (9th Cir. 2006) (en banc) (discussing the history of the case, in which a French prosecutor charged Yahoo! with maintaining on a US Web site material protected under the First Amendment but illegal under French law).

76. *See, e.g.*, Cybersky, Oberlandesgericht [OLG] [Hamburg Ct. App.] Feb. 8, 2006, docket number 5 U 78/05, at juris online/Rechtsprechung (liability can be premised on a causal connection between the ISP and the illegal content, even though the content was posted by a third party acting autonomously).

77. *See, e.g.*, Viaticum/Luteciel v. Google France, Tribunal de grande instance [T.G.I.] [ordinary court of original jurisdiction] Nanterre, 2e ch., Oct. 13, 2003, RG No. 03/00051

holding Internet intermediaries criminally liable for IP infringement that occurs on their systems.[78] Even if we rationalize U.S. safe harbors, therefore, intermediaries will still face unreasonable liability outside the United States. To help solve this problem, Congress and the Administration should press for treaty commitments creating international safe harbors along the lines of a rationalized U.S. safe harbor. Without some form of international protection, intermediaries will face unreasonable risks of liability abroad.

CONCLUSION

Internet intermediaries need safe harbors. In the United States, they have such safe harbors for most – though not all – tort claims. But those safe harbors vary widely in their efficacy, sometimes providing too much protection and sometimes too little, and the patchwork quilt of protections leaves significant holes. A single, rationally designed safe harbor based on a modified trademark model would not only permit plaintiffs the relief they need while protecting Internet intermediaries from unreasonable liability, but would also serve as a much needed model for courts in the rest of the world, which have yet to understand the importance of intermediaries to a vibrant Internet.

(holding Google liable for letting advertisers run ads opposite generic terms "flight market" and "travel market" that the plaintiff claimed as trademarks) (appeal pending).

78. *See* Paul Meller, *EU Weighs Copyright Law*, PC WORLD, Mar. 20, 2007, http://www.pcworld.com/printable/article/id,129995/printable.html (discussing EC draft law).