

Who is Safe in This Harbor? Rethinking Section 230 of the Communications Decency Act

T. Barton Carter, Professor of Communication and Law, Boston University

Legislative bodies and courts have long struggled to reconcile two sometimes conflicting interests: the state's interest in protecting the reputations of its citizens and society's interest in free and robust debate. For example, the constitutional privilege in libel is an attempt to strike a balance between these interests. The evolution of the privilege reflects changing views regarding what constitutes a proper balance.

The advent of the Internet created a different but related problem. The First Amendment interest in the balance was no longer related to a specific type of content, but rather a specific medium of expression. Instead of a concern that defamation law could have a chilling effect on "uninhibited, robust, and wide-open"¹ debate on public issues, the concern was that defamation law, as well as indecency law, privacy law, etc., would chill the development of the Internet.

To address this problem, Congress enacted a safe-harbor provision as part of the Communications Decency Act.² Section 230 provided in part that "No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider."³

In the decade following passage of § 230, the Internet has developed into a major communication medium. It is now pervasive in our society, having a major impact on business, education, entertainment and social interaction.

However, this has not come without some cost. Just ask Kenneth Zeran, Christianne Carafano, the two female Yale law students now suing Autoadmit.com or, most recently, many of the students discussed on Juicycampus.com. They, among others, would almost certainly argue that the cost was too great.

¹ New York Times v. Sullivan, 376 U.S. 254, 270 (1964).

² Communications Decency Act of 1996, Pub. L. No. 104-104 – Feb. 8, 1996, 110 Stat. 133 (1996).

I.

For many years, defamation was considered to be outside the reach of the First Amendment.⁴ Then, in 1964 the Supreme Court extended limited First Amendment protection to defamation in its landmark decision in *Times v. Sullivan*⁵. The Court began by noting “a profound national commitment to the principle that debate on public issues should be uninhibited, robust, and wide-open, and that it may well include vehement, caustic, and sometimes unpleasantly sharp attacks on government and public officials.” The Court found that defamation law, even with the defense of truth available, could have a serious chilling effect on would-be critics of government conduct due to the difficulty and/or expense of proving the truth of their statements.

To reduce this chilling effect, the Court created a constitutional rule requiring public officials to prove actual malice as a prerequisite to receiving damages for a defamatory falsehood regarding their official conduct. The purpose of this rule was to provide adequate breathing space for discussion of public affairs, while protecting public officials from deliberate falsehoods.

After *Sullivan*, several decisions expanded the rule to cover public figures and those who were involved in a matter of public concern. In these cases the Court struggled with the question of exactly where to draw the line leading to plurality decisions that provided lower courts with little guidance.⁶

Finally, the basic parameters of the constitutional privilege in defamation were established in *Gertz v. Robert Welch, Inc.*⁷ The Court began by describing two important societal interests: the First Amendment interest in robust and open debate and the state interest in

³ 47 U.S.C. § 230.

⁴ See, e.g., *Chaplinsky v. New Hampshire*, 315 U.S. 568, 571-572 (1942), “There are certain well-defined and narrowly limited classes of speech, the prevention and punishment of which have never been thought to raise any Constitutional problem. These include the lewd and obscene, the profane, the libelous, and the insulting or ‘fighting’ words”

⁵ 376 U.S. 254 (1964).

⁶ See *Rosenbloom v. Metromedia, Inc.*, 403 U.S. 29 (1971); *Curtis Publishing Co. v. Butts*, 388 U.S. 130 (1967).

⁷ 418 U.S. 323 (1974).

protecting its citizens from wrongful harm to their reputations. It acknowledged that “[s]ome tension exists between the need for a vigorous and uninhibited press and the legitimate interest in redressing wrongful injury.”⁸ The Court’s balance created two classes of defamation plaintiffs: public officials/figures and private individuals.

The advent of the Internet raised new questions regarding the chilling effect of defamation law, as well as privacy law and restrictions on indecent material.⁹ Here the concern was not one of chilling specific content, but rather the development of new services. One of the strengths of the Internet is that it allows individuals to communicate with a worldwide audience at minimal cost. However, if the Internet Service Providers (ISPs) and websites that carry these messages could be held legally responsible for the content, there would be a strong incentive to limit those messages.

With traditional media, liability for other people’s content is determined by distinguishing publishers from distributors. Those who actively choose content, e.g., newspapers, broadcasters, etc., are viewed as publishers and, as such, liable for that content. Passive distributors such as news vendors, bookstores and libraries, are not responsible unless they can be shown to have specific knowledge of the content at issue.¹⁰

Early cases involving interactive computer services applied this traditional distinction. When the publisher of *Skuttlebut*, an electronic newsletter, sued CompuServe for allegedly defamatory statements carried in *Rumorville, USA*, a competing newsletter, the district court held that CompuServe was a distributor and thus not liable. The court found that CompuServe was “in essence” an electronic, for-profit library with “little or no editorial control.”¹¹

However, when a securities investment firm and its president sued Prodigy for a message posted on one of Prodigy’s electronic bulletin boards by an unknown user that called the

⁸ *Id.* at 342.

⁹ Civil liability for invasion of privacy and criminal liability for indecent material each raise different questions. For a general discussion of why a single regulatory scheme covering all liability for websites and Internet Service Providers (ISPs) is not advisable see pp. __, *infra*.

¹⁰ E.g., Barry J. Waldman, *A Unified Approach to Cyber-Libel: Defamation on the Internet, A Suggested Approach*, 6 RICH. J.L. & TECH. 9, 33 (1999).

president a criminal and accused the firm of fraud, a different result obtained. Relying on Prodigy's use of human monitors and automated systems to remove objectionable content, the trial judge held that Prodigy was a publisher and thus could be held liable for the defamatory statements.¹²

The implication of these early cases was that exercising any editorial control over content posted on site would make the website operator or ISP a publisher, and thereby responsible for all the content. This seemed to leave two ways to avoid liability. Website operators and ISPs would either have to exercise editorial control over every line of content posted on their site or not exercise any control at all.

There were two major problems with this result. The first was the obvious chilling effect on the development of new Internet and interactive computer services. Anyone wishing to exercise any editorial control over content posted by others would have to implement a system of full editorial control. Such editorial control would be expensive and time-consuming. It would also require serious limits on the volume of material that could be posted. Without limits, the sheer volume that many services would generate would preclude exercising editorial control.

The second problem was that deterring operators from exercising any editorial control at all would almost certainly increase the amount of objectionable material available. An operator would not remove some objectionable material for fear of then being liable for any that was not removed.

II

In 1996 Congress addressed this problem in § 230 of the Communications Decency Act, part of the 1996 Telecommunications Act.¹³ Congress found that the Internet had “flourished to the benefit of all Americans, with a minimum of government regulation,”¹⁴ and that it is “the policy of the United States . . . to preserve the vibrant and competitive free market that presently

¹¹ *Cubby, Inc. v. Compuserve, Inc.*, 776 F.Supp. 135 (S.D.N.Y.1991).

¹² *Stratton-Oakmont, Inc. v. Prodigy Services Co.*, 1995 WL 323710 (N.Y.Sup.1995).

¹³ Telecommunications Act of 1996, Pub. L. No. 104-104 – Feb. 8, 1996, 110 Stat. 56 (1996).

¹⁴ 47 U.S.C. § 230(a)(4)

exists for the Internet and other interactive computer services, unfettered by Federal or State regulation.”¹⁵

In addition to preventing the specter of tort and/or criminal liability from chilling Internet speech, § 230 was also intended to encourage operators of interactive computer services to remove at least some objectionable speech and to develop filtering tools that would help parents prevent their children from accessing objectionable material.¹⁶ Providing immunity regardless of any exercise of editorial control, was intended to remove the chilling effect caused by decisions like *Stratton-Oakmont*. Ideally, this would reduce the amount of objectionable content disseminated via the Internet and interactive computer services.

Since § 230 was enacted courts have continually interpreted "interactive computer service" broadly. The Statute defines "interactive computer service" as “any information service, system, or access software provider that provides or enables computer access by multiple users to a computer server, including specifically a service or system that provides access to the Internet and such systems operated or services offered by libraries or educational institutions.”¹⁷ Despite arguments that this limited immunity to ISPs and others that provide direct access to the Internet, courts have consistently ruled that it includes websites and listserves as well.¹⁸

Not all objectionable material is covered by § 230. There is an exception for intellectual property. Copyright has a different safe harbor. Unlike § 230, the Digital Millennium Copyright Act (DMCA) does not provide unconditional immunity for interactive computer services. Instead, immunity can be forfeited for failure to comply with the "notice and takedown"

¹⁵ 47 U.S.C. § 230(b)(2)

¹⁶ “It is the policy of the United States ... to remove disincentives for the development and utilization of blocking and filtering technologies that empower parents to restrict their children's access to objectionable or inappropriate online material.” 47 U.S.C. § 230(b)(4).

¹⁷ 47 U.S.C. § 230(f)(2).

¹⁸ See e.g., *Batzel v. Smith*, 333 F.3d 1018, 1030 (9th Cir.2003) (website and listserves are "interactive computer services"); *Carafano* at 1125 (online dating service is an "interactive computer service"); *Gentry v. eBay, Inc.*, 99 Cal.App.4th 816, 831 & n. 7, 121 Cal.Rptr.2d 703 (2002) (on-line auction website is an “interactive computer service”); *Schneider v. Amazon.com*, 108 Wash.App. 454, 31 P.3d 37, 40-41 (2001) (on-line bookstore Amazon.com is an “interactive computer service”); *Barrett v. Clark*, 2001 WL 881259 at *9 (Cal.Sup.Ct.2001) (newsgroup considered an “interactive computer service”).

provisions of the DMCA.¹⁹ Under these provisions, an ISP or website that receives proper notice of infringing material must remove it expeditiously or lose its immunity. There are additional notification requirements to ensure that the posting party has an opportunity to contest an assertion of infringement.²⁰

Trademark law has its own safe harbor. Section 1114(2) of the Lanham Act provides immunity for paid advertising content to publishers and distributors including electronic communications.²¹ Remedies enforceable against the publishers and distributors are limited to injunctions against future publication of the infringing material.²² Immunity in other intellectual property actions ranging from patent law to state right of publicity actions is less clear.²³

III.

In the decade since the passage of the Communications Decency Act, the Internet has grown exponentially. Many new services, not even envisioned at the time § 230 was passed, have become commonplace. These include video services like YouTube, social networking services like Facebook and MySpace and graphically rich multiplayer games like World of Warcraft. Although other factors including the increased availability of broadband²⁴ have also contributed to this increase, there is little doubt that the various safe harbor provisions including § 230 have been a major factor in this growth. Access to the Internet is now seen as essential as universal telephone service.²⁵

However, this has not come without a cost. Individual citizens who have suffered great harm resulting from material posted on the Internet have found themselves without recourse, most often because they cannot identify the posters, while the operators of the web sites or

¹⁹ 17 U.S.C. § 512(c).

²⁰ *Id.*

²¹ 15 U.S.C. § 1114(2)(2000).

²² *Id.*

²³ Mark Lemley, *Rationalizing Internet Safe Harbors*, 6 J. TELECOMM. & HIGH TECH. L. 101, 107 (2007).

²⁴ For example, YouTube is estimated to have consumed as much bandwidth in 2007 as the entire Internet did in 2000. Lohr, Video Road Hogs Stir Fear of Internet Traffic Jam, <http://www.nytimes.com/2008/03/13/technology/13net.html?ei=5065&en=765ff5f673bfdfee&ex=1206072000&partner=MYWAY&pagewanted=print> last visited on March 13, 2008.

²⁵ See Demographics of Internet Users, http://www.pewinternet.org/trends/User_Demo_2.15.08.htm (last visited March 18, 2008).

electronic bulletin boards are protected by § 230. An early example was *Zeran v. America Online, Inc.*²⁶. A message was posted on an AOL bulletin board advertising “Naughty Oklahoma T-Shirts.” The shirts featured offensive slogans referring to the Oklahoma City bombing. The “ad” directed people to call Ken at a phone number which was Kenneth Zeran’s home phone number in Seattle, Washington. The person who posted this was never identified.

After receiving a large number of abusive phone calls, including some death threats, Zeran contacted AOL and the ad was eventually removed, although AOL refused Zeran’s request to have a retraction posted. Subsequently, a number of additional postings similar to the original were placed on the bulletin board leading to an ever-increasing number of abusive phone calls and death threats. The situation was exacerbated a week later when an announcer for an Oklahoma City radio station read one of these “ads” over the air and urged listeners to call the phone number in the ad. It was only after the radio station apologized on air and an Oklahoma City newspaper ran a story on the hoax that the call volume decreased.²⁷

Zeran sued AOL but lost on the ground that § 230 provided AOL full immunity. He was unable to identify the person or persons who actually posted the hoax ads leaving him with no remedy for the harm he suffered.

Similarly Christianne Carafano, an actress who used the stage name Chase Masterson, found herself without recourse when someone created a fake profile for online dating service, Matchmaker. The profile for Chase529 said that she "was looking for a 'hard and dominant' man with 'a strong sexual appetite' and that she 'liked sort of be []ing controlled by a man, in and out of bed.'" E-mailing an address supplied in the profile triggered an automatic reply containing Carafano's home address and phone number. Even though the profile was removed promptly once Matchmaker, which subsequently changed its name to Metrosplash, was contacted by Carafano’s assistant, Carafano received numerous obscene phone calls and letters, as well as a "highly threatening and sexually explicit fax that also threatened her son."²⁸

²⁶ 129 F.3d 327 (4th Cir.1997).

²⁷ *Id* at 329.

Carafano sued Metrosplash for defamation, invasion of privacy and negligence. The district court held that Metrosplash was not entitled to § 230 immunity because the company provided part of the content—the questionnaire used to generate the profiles. However, it granted summary judgment on the privacy claim on the grounds that her address was newsworthy and on the other claims because the company had not acted with actual malice.²⁹ The court of appeals reversed the ruling on § 230 immunity, holding that the questionnaire merely facilitated the provision of content, rather than providing any. The court went on to say, "[f]urther, even assuming Matchmaker could be considered an information content provider, the statute precludes treatment as a publisher or speaker for 'any information provided by *another* information content provider.' 47 U.S.C. § 230(c)(1) (emphasis added). The statute would still bar Carafano's claims unless Matchmaker created or developed the particular information at issue."³⁰

The Carafano case is an early example of how the development of social networking sites has increased the potential harm exponentially. More recently, two Yale law students sued an official of Autoadmit, a college discussion board, as well as various anonymous posters, for false claims regarding one or both, including being infected with sexually transmitted diseases, drug use, bribing Yale officials to gain admission and forming a lesbian relationship with a Yale administrator. Threats of rape were also posted, as well as ones urging readers to contact potential employers with the various allegations that had been posted. When contacted, the Autoadmit administrators refused to remove the posts.³¹

Subsequently, the Autoadmit official was dropped from the suit. The court has ordered expedited discovery in the form of subpoenas to three Autoadmit officials seeking any information that will help identify the 39 anonymous posters who have been sued under the pseudonyms they used for Autoadmit posts.³²

²⁸ Carafano v. Metrosplash.com, Inc., 207 F.Supp.2d 1055 (C.D.Cal.2002).

²⁹ *Id.*

³⁰ Carafano v. Metrosplash.com, Inc., 339 F.2d 1119, 1125.

³¹ Doe v. Ciolli, Case No. 307CV00909 CFD (Conn.2007).

³² Amir Efrati, "Subpoenas Allowed in AutoAdmit Suit", blogs.wsj.com/law/2008/01/30/subpoena-allowed-in-autoadmit-suit/ (last visited March 10, 2008).

The most recent example, and one that arguably takes the problem to a new level is JuicyCampus.com. The basic purpose of this site is to encourage the anonymous posting of gossip regarding people at various college campuses. The postings can be organized by campus and readers can reply, as well as voting on whether the posting is juicy or not. One could characterize the site as bathroom stall walls posted to the Internet. The majority of postings, while not actionable are indecent and mean-spirited. Some, however, are clearly defamatory. These include accusations of rape, sexual deviancy, drug use and alcoholism.

The site has come under heavy criticism at some of the campuses it covers with student leaders at some even calling for a ban on the site. For example, the student government council at Pepperdine voted 23-5 to request such a ban.³³ Similarly, student leaders at Vanderbilt drafted a letter criticizing the site and asking students not to use it.³⁴

What separates Juicycampus.com from the earlier examples is that each of the other sites provided a forum for discussion of other issues, or in the case of Metrosplash, a service that many found valuable, as opposed to existing solely to encourage gossip. In addition, Juicycampus.com promises total anonymity and provides links to anonymizing services. This emphasis on providing anonymity can only serve to encourage the posting of more objectionable material.

IV

The above examples indicate that the balance between encouraging the development of the Internet and protecting individuals' reputations has swung too far in the direction of the former. How could § 230 be amended to better protect individuals' reputations without overly chilling Internet speech?

If the current approach to liability for online defamation is to be modified, the first question is whether to craft an approach specifically for defamation or one that covers other objectionable content as well. Most proposals for changing safe-harbor law start by questioning

³³ Justin Pope, "Students fume at college gossip site," USA Today, http://www.usatoday.com/tech/webguide/internetlife/2008-02-18-juicycampus_N.htm (last visited 3/6/2008).

³⁴ Sara Gast, "Student leaders speak out against JuicyCampus.com," www.insidevandy.com/drupal/node/6591 (last visited March 10, 2008).

the disparity between the treatment of material that infringes intellectual property rights and other objectionable material.

For example, as a prelude to his proposal to replace the various safe harbor provisions with a single one modeled on trademark law,³⁵ discussed *infra*, Stanford Law Professor Mark Lemley presents four major reasons why a unified approach is desirable.³⁶ The first is that "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." A second reason is that the complexity of multiple safe harbors can confuse intermediaries and lead to assume they have immunity in situations where they do not. Similarly, confused plaintiffs may file suits with no merit or forego meritorious ones.

His third argument is that the scope of the intellectual property exception to § 230 is unclear.

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, and even less confident for the penumbra of quasi-IP claims. Cases in this latter category area include the doctrines of misappropriation, idea submission, and state moral rights claims. If all these claims are in fact IP claims, as the First Circuit has assumed, 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, the absolute immunity of section 230 protects intermediaries.

Finally, Lemley contends that the different protections afforded different content can lead to litigation abuses with plaintiff's mischaracterizing claims as IP for the express purposes of removing them from § 230 immunity or the separate treatment afforded trademark claims.

³⁵ Lemly.

³⁶ It should be noted that Professor Lemley is lead counsel for the two Yale Law Students in the Autoadmit case.

At first blush, these arguments appear persuasive. However, they fail to take into account three major issues. The first is the distinction between the types of harm that can result from different content. For example, copyright infringing material can cause economic harm to the copyright holder, but it is unlikely to cause reputational harm or emotional distress the way defamatory or privacy infringing material can. Indecency law presents still different issues as it is usually justified in terms of protecting children.³⁷

The second major issue is how different types of content are treated under the First Amendment, in terms of both liability and potential remedies. Conflicts between copyright law and the First Amendment are resolved by the idea/expression of the idea dichotomy.³⁸ Among other things, this means that an injunction is treated the same as any other copyright remedy,³⁹ whereas when applied to other content restrictions it is considered a prior restraint.⁴⁰ As noted above, defamation, for many years held to be devoid of First Amendment protection, is now protected under the *Gertz* test.⁴¹ There are even different types of protection for different branches of invasion of privacy.⁴² As far as indecency law is concerned, the First Amendment analysis even differs based on the medium of transmission.⁴³

The final major issue involves the current or potential availability of technological solutions to the problems caused by different forms of objectionable content—specifically filtering technologies. One of the claims made by Viacom in its copyright infringement suit against Google, owner of YouTube, is that Google is using filtering technology to identify and possibly remove copyright infringing material, but only on behalf of those copyright holders who agree sign a licensing agreement with Google.⁴⁴ Similarly, one of the key factors in the various

³⁷ See, e.g., *Ashcroft v. ACLU*, 542 U.S. 656; *Reno v. ACLU*, 521 U.S. 844 (1997); *FCC v. Pacifica Foundation*, 438 U.S. 726 (1978).

³⁸ See *Harper & Row Publishers, Inc. v. Nation Enterprises*, 471 U.S. 539 (1969).

³⁹ See *Salinger v. Random House, Inc.*, 811 F.2d 90 (2d Cir. 1987).

⁴⁰ See *New York Times Co. v. United States*, 403 U.S. 713 (1971); *Near v. Minnesota*, 283 U.S. 697 (1931).

⁴¹ *Gertz*.

⁴² E.g., *Time, Inc. v. Hill*, 385 U.S. 374 (1967), *Florida Star v. B.J.F.*, 491 U.S. 524 (1989).

⁴³ *Pacifica Foundation*, 438 U.S. at 737-38; *Reno*, 521 U.S. at 877-80; *Cohen v. California*, 403 U.S. 15, 19 (1971).

⁴⁴ *Viacom Intern. Inc. v. YouTube, Inc.*, No. 07 CIV. 2103 (S.D.N.Y.2008)

court decisions involving Internet indecency statutes has been the degree to which filtering programs represent a solution to the problem that is less restrictive of First Amendments rights.⁴⁵

This does not mean that some solutions to the problem might not be appropriate for all objectionable content, but rather that one should not start with the assumption that one size fits all. Of the two changes I propose, one is appropriate for all forms of objectionable content, but the other is specifically tailored to defamation.

V.

Before turning to my proposal it is useful to look at other proposed solutions. Lemley has identified four possible approaches. These are eliminating safe harbors either entirely or for specific content, extending the absolute immunity of § 230 to intellectual property, extending the DMCA "notice and takedown" provisions to other content or his proposal to apply a modified version of trademark law to all content.

In terms of the first, Lemley correctly argues that "[i]t 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."⁴⁶ There is no question that the potential liability would cause all website operators to drastically limit third-party content.⁴⁷ Even ISPs that could theoretically pass the costs on to consumers would be deterred from offering access to anything other than trusted sites because the rates they would have to charge to cover potential liability would be prohibitive. This would be true even if safe-harbor immunity were removed only for defamation actions.

The second approach, extending § 230 to other types of content such as copyright, would not change the current law regarding defamatory content. Thus, there is no need to discuss it further.

⁴⁵ *Ashcroft*, 542 U.S. at 666-670.

⁴⁶ Lemley at 112

Turning to the third approach, extending the "notice and takedown" provisions of the DMCA to other content including defamatory statements, Lemley notes several problems, but only one is of particular relevance in the context of defamatory content. In the copyright area, "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."⁴⁸ There are studies indicating that a large percentage of "notice and takedown" complaints are frivolous,⁴⁹ and that despite provisions designed to allow posters to contest these frivolous complaints and have their content reposted, this almost never happens.⁵⁰

Extending "notice and takedown" provisions to defamation would have the same effect, only worse. The use of defamation actions to silence critics has been so common as to be given its own title, Strategic Litigation Against Public Participation, (SLAPP) and have anti-SLAPP statutes passed for the specific purpose of curbing the practice.⁵¹

Furthermore, "notice and takedown" would not necessarily be of great benefit to defamed individuals. Often, by the time defamatory material is brought to the attention of the person it defames the reputational damage is done. Simply removing it from the site does not repair that damage.

Finally, there is Lemley's proposal, an approach based on trademark law. He argues that extending the trademark approach to other content would have the following advantages:

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.

⁴⁷ *Ashcroft*, 542 U.S. at 670; *Reno*, 521 U.S. at 882.

⁴⁸ Lemley at 118.

⁴⁹ 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 COMP. & HIGH TECH. L.J. 621 (2006).

⁵⁰ *Id.*

⁵¹ See, e.g., Cal.Civ.Proc.Code § 425.16.

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 injunction removing offensive content. 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, 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.⁵²

The best feature of his proposal as applied to defamation would be giving defamed individuals the ability to identify the original posters of the defamatory material so that they can take legal action against them. However, injunctive relief is not well-suited to defamation actions. As previously discussed, removing the material, especially after a lengthy period of time, is often of little benefit to a defamation victim as the harm has already occurred. If it would only be taken down after litigation, it would render the relief almost meaningless. Even if the result of a dispute resolution process, it would be too little, too late.

A second problem is that injunctive relief might well run into constitutional problems. As noted above, an injunction applied to speech is considered a prior restraint. Prior restraints

⁵² Lemley at 119 (footnotes omitted).

carry a strong presumption of unconstitutionality placing a heavy burden on the government to justify them.⁵³ For this reason, injunctions for defamation are almost never permitted.⁵⁴

VI.

A better approach combines one feature of Lemley's proposal that does seem to have applicability to a wide range of content and legal actions with an additional component applicable solely to defamation. Specifically, it would limit anonymity, while providing defamed individuals with a right of reply.

Lemley is correct in identifying the widespread ability to post anonymous content as one of the basic problems. One of the key problems with the current system is the degree to which it encourages anonymous speech. This is not to say that anonymous speech is always bad. In fact, there are many situations where anonymous speech serves society and needs to be protected.

“Anonymous pamphlets, leaflets, brochures and even books have played an important role in the progress of mankind.”⁵⁵ Recognizing the importance of anonymous political speech, the Supreme Court has held it to be protected by the First Amendment.⁵⁶ Regulations that restrict anonymity in the area of core political speech are unconstitutional unless they are “narrowly tailored to serve an overriding state interest.”⁵⁷

Similarly, reporters' rights to protect the identity of confidential sources are based in the belief that sources would otherwise be deterred from providing reporters with information.⁵⁸

However, it is hard to equate the defamatory material in *Zeran*, *Carafano*, and the *Autoadmit* case, or that posted on *Juicycampus.com*, with either of those examples. As long as

⁵³ *Bantam Books, Inc. v. Sullivan*, 372 U.S. 58, 70 (1963).

⁵⁴ *But see* *Tory v. Cochran*, 544 U.S. 734, 738 (2005).

⁵⁵ *Talley v. California*, 362 U.S., at 64, (1960).

⁵⁶ *Talley, McIntyre v. Ohio Elections Com'n*, 514 U.S. 334 (1995).

⁵⁷ *McIntyre*, 362 U.S. at 347.

⁵⁸ See e.g., Vincent Blasi, *The Newsman's Privilege: An Empirical Study*, 70 Mich.L.Rev. 229 (1971).

the regulation is narrowly tailored to serve the overriding state interest in protecting its citizens' reputations, it should survive constitutional scrutiny.

Restricting the ability to post anonymous defamatory statements would serve two state interests. First, it provides a legal remedy for defamed individuals by identifying the original publisher of the defamation, thus allowing them to be sued. Section 230 has created the catch-22 of preventing defamation victims from suing the publishers they can identify (e.g., the website operators), while at the same time leaving them unable to identify those that they can sue (the original poster).

However, the ability to identify and then sue has limited value. First, money cannot restore a damaged reputation. Second, because of the constitutional protection afforded by *Sullivan* and *Gertz*, it is difficult for even a falsely defamed individual to win a defamation case. Third, the Internet has drastically changed a key dynamic. Previously, there was at least some correlation between the ability to seriously damage a reputation and the financial status of the publisher. Widespread dissemination of a defamatory statement generally occurred in a newspaper, book, magazine or broadcast station, all of which required extensive financial resources. Thus, a successful libel suit held out the promise of collecting a significant sum of money which could justify the time and expense involved in bringing the defamation action. In contrast, the Internet allows anyone to widely distribute defamatory statements at a negligible cost leading to a likelihood that even a successful defamation suit may ultimately provide little or no compensation.

Far more important would be the deterrent effect. Posters who know that they can be identified and sued for their statements are far less likely to post actionable statements. The biggest problem with sites such as Juicycampus.com is that they actively encourage irresponsible postings by ensuring that there cannot be any negative consequences for whoever posts them.

The key then, is to find a way to limit anonymous defamatory speech, while at the same time protecting other anonymous speech. There are two parts to this. First, those granted § 230 immunity must be required to obtain identifying information on posters, and retain that

information for a reasonable period of time. A relatively simple way to accomplish that would be conditioning immunity on obtaining and retaining that information. Of course, it would not guarantee the ability to identify all posters, as there are steps posters can take to conceal their identities.⁵⁹

The more difficult question is when, and under what circumstances, would an allegedly defamed individual be able to obtain the identity of the poster. If it is too easy to compel disclosure, there is the danger that speakers who are entitled to anonymity will lose it. On the other hand, if it is too difficult to obtain the identity, the provision could arguably lose any value.⁶⁰

As part of his proposal to use a trademark model for all online safe harbor, Lemley proposes a system "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 [an arbitration proceeding.]"⁶¹

The primary danger here is defining "good cause" and determining how good a showing would be required. There is a real danger that the bar would be set too low, resulting in inadequate protection for legitimate anonymous speech. Given the First Amendment interest at stake, the DMCA approach requiring a suit to be filed before issuing the subpoena better balances the competing interests. Once the subpoena is issued, the anonymous poster should be notified and given the chance to contest the subpoena, including offering proof of any defenses or privileges that would preclude a verdict for the plaintiff. If the subpoena is contested the plaintiff should be forced to demonstrate a likelihood of winning on the merits before disclosure of the defendant poster's identity could be compelled. This approach has already been used in Internet defamation cases.⁶²

⁵⁹ For example, 'anonymizers' are various types of software that prevent the discovery of an Internet user's IP address by creating an encrypted path between the user's computer and the Internet.

⁶⁰ The same problem is raised by defamation cases where the defendant relied on anonymous sources. Forcing the reporter to immediately reveal sources encourages the filing of spurious suits for the express purpose of identifying the source of any uncomplimentary story. On the other hand, allowing the source to remain anonymous throughout the case may make it impossible to prove negligence and/or actual malice as required by *Gertz*.

⁶¹ Lemley, *supra* note 24 at 117

⁶² See e.g., *Dendrite International Inc. v. Doe No. 3*, 342 N.J.Super. 134 (2001).

Although this may seem to place too great a burden on the defamation plaintiff, it does not require any more than what would be necessary to win such a lawsuit. Furthermore, the threat of litigation costs even prior to disclosure would serve as a significant deterrent to defamatory postings. In addition, this relatively high bar to compelled disclosure would provide strong protection for anonymous speech and increase the likelihood of it being viewed as narrowly tailored to serving the overriding state interest.

There is, however, another way to reduce the harm in at least some cases. One of the classic First Amendment aphorisms is, "the remedy for speech is more speech."⁶³ In this context more speech would come in the form of a right of reply.⁶⁴ Specifically, upon receiving a complaint that an allegedly defamatory statement has been posted, a website operator would be required to post a response from the individual who claims to have been defamed.⁶⁵ The response would have to appear in the same screen with the original statement so that anyone viewing the original statement would be exposed to the response as well.

Failure to comply would result in the loss of § 230 immunity.

Given that a defamed individual might conclude that a reply would be ineffective and thus prefer that the original post be removed there would also be another option. If both the website operator and the allegedly defamed individual agree to remove the original post instead, there would be no obligation to post the reply. Neither party should be able to opt for this alternative unilaterally. Allowing those who claim to be defamed to do so would allow them to too easily silence critics through questionable defamation claims.⁶⁶ Allowing the website operator to do so might deprive a defamed individual of the only effective remedy.

⁶³ See, e.g., *Whitney v. California*, 274 U.S. 357, 377 (1927).

⁶⁴ A similar result might be obtained through some form of retraction statute, but retraction does not make sense when applied to a website operator who had nothing to do with creating the defamatory statement and who most likely has no way of knowing whether the statement is true or false.

⁶⁵ This remedy is limited to defamation. It could arguably be extended to false light invasion of privacy, but would be of little value in other areas of privacy such as public disclosure of embarrassing facts or right of publicity. For an extensive discussion of privacy and the Internet, please see Daniel Solove, *The Future of Reputation: Gossip, Rumor and Privacy on the Internet*, Yale University Press, New Haven, Conn., 2007.

⁶⁶ This is essentially the same problem that exists with a "notice and takedown" system. See discussion pp. ____, *supra*.

From the standpoint of the defamed individual, this remedy would have several advantages over the current system. Obviously, the primary concern of a defamed individual is limiting the reputational harm caused by a defamatory statement and then repairing the damage that has been done. The traditional solution has been to sue for defamation. A successful libel suit accomplishes two things, undoing the harm through a court determination that the statement was false and providing compensation for the harm suffered.

Unfortunately, there are a number of problems with this solution. First, to erase or overcome the harm done, the court finding would have to be disseminated to all those who were exposed to the original defamatory statement. Realistically, this is impossible. Second, to be effective, the rebuttal of a defamatory statement must appear soon after the first appearance of the statement itself. Otherwise, people's opinions tend to become fixed and the diminished reputation firmly established. Third, assessing harm to reputation and determining adequate compensation is difficult. Fourth, when there is recovery, it does not occur until years after the original injury. Fifth, due to the immunity of the website and the inability to determine the original poster, the defamed individual is often left with no one to sue.⁶⁷

In contrast, a reply could be posted immediately, thus giving the allegedly defamed individual a chance to minimize the harm done by the original statement. Note, for example, in the *Zeran* case, that once a newspaper published a story on the hoax, the threatening phone calls were reduced to a fraction of their previous volume.⁶⁸ One can surmise that had that information been available sooner, the radio station announcer would have been far less likely to urge listeners to call *Zeran* a week after the original posting.

Linking the reply to the statement on the same site also would make sure it is distributed to any new readers of the statement. Any individual who returns to that page would also see the reply.

⁶⁷ Although the other proposed change, requiring sites to obtain and retain identifying information would reduce this problem, there will still be posters who are able to conceal their identity. In addition, due to the global nature of the Internet there can be serious jurisdictional and logistical issues that would preclude suing the original poster.

⁶⁸ *Zeran*, 129 F.3d at 329.

Of course, the effectiveness of a right of reply would vary from case to case. Sometimes the damage is so immediate that it can't be remedied by either a response or removal of the material. In *Carafano*, even though the material was removed almost immediately, serious harm resulted.⁶⁹ It is hard to see how any response posted would have done anything to reduce the harm.

Another advantage of the right of reply is that it imposes minimal cost on the website operator. Rather than getting involved in litigation over the removal of the original post, all that is required is posting the reply.

Finally, when compared to any remedy that focuses on removing the defamatory material, it reduces the opportunity for the heckler's veto. As previously discussed, one of the big problems with the "notice and takedown" provisions of the DMCA is the ability of someone who wants to material removed to make a false copyright claim regarding that material. Giving the website operator a low-cost alternative to removing the material reduces the likelihood someone will be able to induce removal by threatening legal action.

There is, of course, the question of whether or not this proposed right of reply option would be constitutional. Right-of-reply laws have met with mixed success in the Supreme Court. The personal attack rule was upheld in *Red Lion v. Federal Communications Commission*.⁷⁰ However, a Florida right-of-reply statute that applied to newspapers was struck down in *Miami Herald v. Tornillo*.⁷¹

These two holdings are generally viewed as setting different constitutional standards for print and broadcasting.⁷² It has long been held that "differences in the characteristics of new media justify differences in the First Amendment standards applied to them."⁷³ Given that, what

⁶⁹ *Carafano*, 339 F.2d at 1122.

⁷⁰ 395 U.S. 367 (1969). Starting in the 1980's many commenters began questioning the continued constitutionality of the rule. It was eventually struck down by the court of appeals in 2000, *Radio-Television News Directors Association v. Federal Communications Commission*, 229 F.3d 269, but on administrative law grounds.

⁷¹ 418 U.S. 241 (1974).

⁷² See *Minneapolis Star and Tribune Co. v. Minnesota Com'r of Revenue*, 460 U.S. 575, 591 (1983) (holding "ink and paper" tax unconstitutional because it singles out newspapers).

⁷³ *Red Lion* 395 U.S. at 387 citing *Joseph Burstyn, Inc. v. Wilson*, 343 U.S. 495 (1952); see also, *F.C.C. v.*

characteristics of the Internet would be relevant to a decision on a right-of-reply rule for the Internet?

When faced with applying the First Amendment to the Internet, the Supreme Court rejected attempts to apply the lower broadcast standard, reasoning that the scarcity rationale underpinning *Red Lion* has no application to the Internet.⁷⁴ A strong argument can be made that the Internet is the least scarce medium in history.⁷⁵ Similarly, the other rationale used to justify more limited First Amendment rights in broadcasting, its pervasiveness and unique accessibility to children,⁷⁶ has been rejected with regard to the Internet.⁷⁷

However, there are characteristics of the Internet that can be argued would affect the constitutionality of a right-of-reply rule applied to the Internet. In *Miami Herald* the primary concern of the Court was that the right-of-reply statute penalized newspapers for printing certain content. "The first phase of the penalty resulting from the compelled printing of a reply is enacted in terms of the cost in printing and composing time and materials and in taking up space that could be devoted to other material the newspaper may have preferred to print."⁷⁸ The Court concluded that this cost would have a chilling effect on newspapers and might deter them from publishing material that would result in a compelled reply.⁷⁹

The Court further reasoned that even if it did not impose any additional costs, the right-of-reply statute was nevertheless unconstitutional "because of its intrusion into the function of editors."⁸⁰ Editors, not the government, should choose what content goes into a newspaper and what is left out.

League of Women Voters of California, 468 U.S. 364 (1984)(Justice Kennedy concurring); *Ashcroft v. American Civil Liberties Union*, 535 U.S. 564 (2002).

⁷⁴ *Reno v. American Civil Liberties Union*, 521 U.S. 844 (1997).

⁷⁵ *Id.* at 870.

⁷⁶ See *Pacifica v. Federal Communication Commission*, 438 U.S. 726 (1978).

⁷⁷ See *Reno* 521 U.S. at 844.

⁷⁸ *Miami Herald*, 418 U.S. at 256.

⁷⁹ *Id.*

⁸⁰ *Id.* at 258.

A right-of-reply statute applied to websites that allow posting of third-party content presents a very different situation. First, the cost of posting the reply is negligible and size limitations do not really exist. Posting a reply will not require removal of other content. Thus, the chilling effect that concerned the Court in *Miami Herald* would not result from this proposed right-of-reply requirement.

As far as the intrusion into editorial decision making is concerned, there is again no similarity to the newspaper model at issue in *Miami Herald*. Section 230 is ultimately rooted in the fact that website operators are incapable of exercising complete editorial control.⁸¹ Website operators are given immunity because it is unreasonable to hold them responsible for content they can't review and control.

VII.

A decade after § 230 was passed, it has become apparent that in the context of defamation law the balance between free speech and protecting individuals' reputations is set too far in favor of free speech. Currently, defamed individuals too often face an untenable situation of being unable to sue those they can identify, while being unable to identify those they could sue.

To remedy this problem, website operators should be required to obtain and retain adequate identifying information from all posters, so that defamed individuals can pursue appropriate legal remedies. At the same time, website operators should, upon request, be required to post an allegedly defamed individual's reply, linked to the original post. Such replies will help defamed individuals minimize the reputational harm caused by the original post.

⁸¹ See *Zeran* 129 F.3d at 330.