9-1-2009

Sex, Lies, and the Internet: Balancing First Amendment Interests, Reputational Harm, and Privacy in the Age of Blogs and Social Networking Sites

Robert D. Richards

Follow this and additional works at: http://scholarship.law.unc.edu/falr
Part of the First Amendment Commons

Recommended Citation
Available at: http://scholarship.law.unc.edu/falr/vol8/iss1/6

This Article is brought to you for free and open access by Carolina Law Scholarship Repository. It has been accepted for inclusion in First Amendment Law Review by an authorized editor of Carolina Law Scholarship Repository. For more information, please contact law_repository@unc.edu.
SEX, LIES, AND THE INTERNET:
BALANCING FIRST AMENDMENT
INTERESTS, REPUTATIONAL HARM, AND
PRIVACY IN THE
AGE OF BLOGS AND SOCIAL
NETWORKING SITES

ROBERT D. RICHARDS*

INTRODUCTION

When Matt Ivester, founder and chief executive of the now-defunct Juicy Campus,1 addressed a packed gathering of Georgetown University students in October 2008—the first time he faced such an audience—he bluntly told the crowd: “The fact is, the Internet is changing privacy as we know it.”2 Amid student concerns that his website, which “encourages people to post gossip anonymously . . . naming names and spreading detailed rumors about sex, drugs, [and] college life,”3 could adversely affect their future careers, particularly those hoping to enter government service, Ivester offered little comfort, telling the group that employers are “going to have to start developing a sense of humor.”4


2. Susan Kinzie, Juice, the Whole Juice and Nothing but the Juice, WASH. POST, Oct. 30, 2008, at B1 (describing JuicyCampus as “the fast-growing gossip Web site . . . that is igniting controversies on campuses across the country.”).

3. Id.

4. Id.
JuicyCampus was a relative newcomer—launched in October 2007—to a growing number of online, anonymous posting opportunities that often provide open invitations to ventilate freely about such things as "the campus' most attractive students, biggest drug users and popular places for illicit sexual activity" or, in the case of blogs outside academic circles, the political battle of the day. In February 2009, Ivester announced that he was shutting down the controversial site, citing declining "ad revenue because of the bad economy" as the reason. Visitors to JuicyCampus were "redirected to a site called College Anonymous Confession Board, whose owner said he hosts 'a higher level of discourse.'"

On college and university campuses, those taking classes are not the only ones who may unwittingly face online wrath. Both satisfied and dissatisfied students can make their feelings known—anonymously, that is—on Rate My Professors, a user-friendly service that enables posters to exalt or excoriate instructors with ease. Such ratings are not limited to higher education. Students and parents similarly may post comments about K-12 teachers on a sister site, Rate My Teachers.

7. Deborah Gage, Internet Chatter Drawing Lawsuits, S.F. CHRON., Feb. 9, 2009, at A1 (noting that "the site also had been scrutinized by several state attorneys general and had some of its posters sued last year by a University of Delaware student who wanted gossip about herself removed from the site").
8. Id.
In addition to blogs, social networking sites—notably MySpace, Facebook, and Twitter—are burgeoning throughout cyberspace. The popularity of these sites perhaps was nowhere more evident than during the 2008 presidential election. As the *Los Angeles Times* reported,

> Without a doubt, the election was a high-water mark for activity on the Web. Not only did news sites see record traffic—latimes.com had its best day ever with more than 8.2 million page views Tuesday—but marquee new media communities such as Twitter, YouTube, Facebook and Digg hummed from morning to night.

The news media clearly are no strangers to the blogosphere and are working on new ways to attract audiences to their websites. While hosting online blogs provides a convenient way for


13. Twitter, http://twitter.com (last visited Sept. 5, 2009) (stating that “[a]t Twitter, we ask one question, ‘What are you doing?’ . . . The result of using Twitter to stay connected with friends, relatives, and coworkers is that you have a sense of what folks are up to”).

14. See generally JOHN PALFREY & URS GASSER, BORN DIGITAL: UNDERSTANDING THE FIRST GENERATION OF DIGITAL NATIVES 1 (2008) (noting that people born after 1980 are “Digital Natives” and, as such, “[t]hey all have access to networked digital technologies. And they all have the skills to use those technologies.”).

15. David Sarno, *The 2008 Election Web Scout; A Logjam of Voting Chatter*, L.A. TIMES, Nov. 6, 2008, at E1 (observing that “[a] generation of Web users was busy taking video, sharing personal stories, offering commentary and generally showing that just watching an election is no longer the optimal way to participate in”).

readers and viewers to connect with the media and each other, it also reveals some useful personal information on which media organizations can base business decisions. As Broadcasting & Cable, a leading trade publication for electronic media, reported in September 2008, "[a]udience listening is possible because social Web sites, chat rooms, e-mail, blogging and other forms of personal expression in digital media are easily data mined." 17

With the proliferation of user-generated content—much of it anonymous—comes a social cost in terms of protecting reputation, privacy, and sometimes even physical safety in an online world. In November 2008, a nineteen-year-old community college student in Pembroke Pines, Florida, committed suicide on a live video website, "’egged on’ by strangers who, investigators say, encouraged him to swallow the antidepressant pills that eventually killed him." 18

That same month a Missouri woman, Lori Drew, was convicted by a federal jury in California of “three misdemeanor counts of computer fraud for having misrepresented herself on the popular social network MySpace.” 19 Drew, pretending to be a teenage boy, first sent “friendly and then menacing messages to Megan Meier, 13, who killed herself shortly after receiving a message in October


18. Brian Stelter, Web Suicide Viewed Live and Reaction Spur a Debate, N.Y. Times, Nov. 25, 2008, at A16 (noting that “[l]ive video of the death was shown online to scores of people, leading some viewers to cringe while others laughed”).

19. Brian Stetler, Guilty Verdict in Cyberbullying Case Provokes Many Questions over Online Identity, N.Y. Times, Nov. 28, 2008, at A28 (suggesting that “[t]here are legitimate reasons to hide one’s name and other information online, be it concern about identity theft or a need for comfort when asking for advice or help”).
2006 that said in part, ‘The world would be a better place without you.’”20 The conviction came under a statute that had “been used almost exclusively to prosecute hacker crimes”21 and rested on the terms of service on MySpace, which require posters, when registering, to be truthful and accurate.

Drew’s conviction has raised the question whether online terms of service agreements, often clicked but largely ignored by users, will become the basis for redefining criminal law. Andrew M. Grossman, a legal policy analyst at the Heritage Foundation, noted at the time of the Drew conviction that the verdict “means that every site on the Internet gets to define the criminal law . . . . What used to be small-stakes contracts become high-stakes criminal prohibitions.”22

Even the judge in Drew’s case was troubled by the way this particular law was applied against her. On July 2, 2009, U.S. District Judge George H. Wu acquitted Drew, because “the federal statute was too ‘vague’ when applied in this case and . . . were he to allow Ms. Drew’s conviction to stand, ‘one could literally prosecute anyone who violates a terms of service agreement’ in any way.”23

With the issue of Internet anonymity bubbling up in courts and legislatures across the country, a showdown between reputation, privacy, and safety interests on the one hand, and the First Amendment rights of message posters and online service providers on the other, is inevitable.

What happens if an anonymous poster on Rate My Professors, MySpace, or a newspaper’s blog levels a defamatory remark or

20. Id.

21. Id. (noting that “Ms. Drew’s creation of a phony profile amounted to ‘unauthorized access’ to the site, prosecutors said, a violation of the Computer Fraud and Abuse Act of 1986”).

22. Id.

23. Rebecca Cathcart, Conviction is Tossed Out in MySpace Suicide Case, N.Y. TIMES, July 3, 2009, at A14 (noting that “the United States attorney in Los Angeles, Thomas P. O’Brien, who brought the case, said a dismissal would leave open the possibility of an appeal”). See also United States v. Drew, 2009 U.S. Dist. LEXIS 85780 (C.D. Cal. Aug. 28, 2009) (granting the defendant’s motion to dismiss the indictment on grounds that the statute was unconstitutionally vague).
invades the privacy of an identifiable person? Should the service itself be held legally accountable? As the law currently stands, the entity that provides the forum, for the most part, is immune from liability flowing from third-party content under § 230(c), the so-called "Good Samaritan" provision, of the Communications Decency Act (CDA). In other words, the law protects those who merely distribute content supplied by others. But the law in this area is not completely settled. In 2008, for instance, two federal courts of appeals differed as to the extent of the immunity that should attach to the Internet Service Provider (ISP).

In Chicago Lawyers' Committee for Civil Rights Under Law, Inc. v. Craigslist, Inc., the Seventh Circuit ruled that the online advertising service Craigslist did not violate federal fair housing laws when it allowed posters to place discriminatory restrictions on offers of housing based upon classifications of race, religion, or gender. Meanwhile, the Ninth Circuit, sitting en banc in Fair Housing Council of San Fernando Valley v. Roommates.com, LLC, found the roommate locator service violated anti-discrimination laws because users answered a preference questionnaire that was provided by the online service—an instrument the court found to elicit information that, in effect, created discriminatory postings. Doing its best to keep ISP protection in place, the court wrote, "[t]he message to website operators is clear: If you don’t encourage illegal content, or design your website to require users to input illegal content, you will be immune." Both cases will be discussed more fully below.

24. Communications Decency Act, 47 U.S.C. § 230(c) (2006). For a discussion of the development and early challenges to the Act, see ROBERT D. RICHARDS, FREEDOM'S VOICE: THE PERILOUS PRESENT AND UNCERTAIN FUTURE OF THE FIRST AMENDMENT 79 (1998) (noting that the Citizen Internet Empowerment Coalition, one of the early legal challengers, "proclaimed that the outcome of this lawsuit 'will likely determine the legal status of speech on the Internet and the future of the First Amendment in the Information Age'").
25. 519 F.3d 666 (7th Cir. 2008).
26. 521 F.3d 1157 (9th Cir. 2008) (en banc).
27. Id. at 1175.
28. See infra notes 87-102 and accompanying text.
Craigslist may have escaped liability in *Lawyers' Committee*, but that case did not end its legal problems. In March 2009, Cook County, Illinois Sheriff Thomas Dart filed a federal lawsuit against the service, claiming that “Craigslist is the single largest source of prostitution in the nation.”\(^\text{29}\) The litigation arose from an unmonitored section of Craigslist advertising “Erotic Services.”\(^\text{30}\) The section contains advertisements for “erotic massage, strippers, [and] escort services.”\(^\text{31}\) Craigslist is expected to raise § 230 as a defense.\(^\text{32}\)

Even if immunity attaches to the ISP, can the third-party poster be held liable for violations of law? The short answer is yes, but there is a dilemma. If the poster is anonymous, can the service provider be forced to reveal identifying information about the poster, thereby undercutting the concept of anonymous speech? That question was an issue of first impression before Maryland’s highest court. The Maryland Court of Appeals heard arguments in December 2008 “[i]n a First Amendment case with implications for everything from neighborhood e-mail lists to national newspapers.”\(^\text{33}\) A Dunkin’ Donuts franchise owner from Maryland’s Eastern Shore alleged that he was defamed by an anonymous comment posted on NewsZap.com that described his store “as one ‘of the most dirty and unsanitary-looking food-service places I have seen.’”\(^\text{34}\) As the *Washington Post* described the oral argument, “[f]or advocates of strong protections for anonymous speech and

---

29. See John Koopman, *Suit Alleges Craigslist Ads Promote Prostitution*, S.F. CHRON., Mar. 6, 2009, at B1 (noting that the sheriff contends that “[m]issing children, runaways, abused women and women trafficked in from foreign countries are routinely forced to have sex with strangers because they’re being pimped on Craigslist”).

30. Id.

31. Id.

32. Id.

33. Henri E. Cauvin, *Maryland Court Weighs Internet Anonymity*, WASH. POST, Dec. 9, 2008, at B1 (noting that the case marks “the first time the Maryland Court of Appeals has confronted the question of online anonymity, an issue that has surfaced in state and federal courts over the past few years as blogs and other online forums have increasingly become part of the national discourse”).

34. Id.
the Internet, online chat rooms are the 21st-century successors to the town square and the political pamphlet."

In February 2009, Maryland’s Court of Appeals ruled that the trial judge “abused his discretion when ordering the identification of the five anonymous Internet forum participants, because the three participants sued, concededly, did not make the alleged defamatory statements, while the other two anonymous participants, who allegedly made the actionable remarks, were not sued by [the plaintiff]."

Without question, courts are grappling with a dizzying array of issues arising out of blogs and social networking sites. As the cases proliferate, courts are beginning to parse the protection according to subtle nuances in fact patterns, which invites the question: just how long will it be before the legal levee breaks and the immunity—prized at least in the view of First Amendment advocates—is narrowed by court interpretation or legislative revision? Such a result would have a profound effect, not only on future online development, but also on First Amendment jurisprudence.

This article examines the legal evolution of online posting through blogs and social networking sites and the simultaneous development of ISP immunity through § 230, concluding ultimately that the area is ripe for reform that should seek to balance personal harms and First Amendment interests. Part I of this article traces the development of ISP immunity under federal law, along with litigants’ attempts to circumvent it in the early stages of the law. Part II examines the rash of recent cases involving questions of third-party postings and suggests that courts may soon grow weary of blanket immunity in light of increasingly egregious fact patterns and calls for reform. Part III analyzes the critical issue whether an ISP can be forced to provide identifying information about its anonymous posters, thus threatening a historical tradition in our national commitment to free speech principles.

35. Id.
37. See infra notes 41-67 and accompanying text.
38. See infra notes 68-102 and accompanying text.
39. See infra notes 103-67 and accompanying text.
cludes in Part IV by suggesting a pragmatic revision of § 230 immunity that balances First Amendment interests with individual rights to redress real injuries through litigation.\textsuperscript{40}

I. SECTION 230: CONSTRUCTING A WALL OF PROTECTION

Prior to CDA § 230, courts were left to apply traditional publisher liability to online content.\textsuperscript{41} A central variable of such liability was how much control the online provider exercised over third-party content. In \textit{Stratton Oakmont v. Prodigy Services Co.}, a New York court ruled that an online service provider acted as a publisher "[b]y actively utilizing technology and manpower to delete notes from its computer bulletin boards on the basis of offensiveness and 'bad taste.'"\textsuperscript{42} In the court’s view, the fact that the service used both technological and human screening of online postings constituted editorial control.\textsuperscript{43}

The court observed:

That such control is not complete and is enforced both as early as the notes arrive and as late as a complaint is made, does not minimize or eviscerate the simple fact that PRODIGY has uniquely arrogated to itself the role of determining what is proper for its members to post and read on its bulletin boards.\textsuperscript{44}

The battle lines were drawn early as to when liability attaches. Post-\textit{Stratton Oakmont}, a series of cases, bolstered by the newly enacted CDA § 230, helped establish the pivotal distinction between a distributor of information and an online publisher. One such case—a $30 million defamation lawsuit—involved a high-level

\textsuperscript{40} See \textit{infra} notes 168–70 and accompanying text.


\textsuperscript{42} \textit{Stratton Oakmont}, 1995 WL 323710, at *4.

\textsuperscript{43} Id.

\textsuperscript{44} Id.
SEX, LIES, AND THE INTERNET

White House official and one of the country’s early leaders in online service.

Sidney Blumenthal, an aide to then-President Bill Clinton, and his wife sued online gossiper Matt Drudge and America Online (AOL) for defamation after Drudge reported falsely that “[n]ew White House recruit Sidney Blumenthal has a spousal abuse past that has been effectively covered up.”

As the Washington Post reported AOL’s position at the time, “[t]he company believes it is protected by language buried deep in Section 230 of the Telecommunications Act of 1996, which states, ‘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.’” The company was correct in its belief. As it turned out, the language of § 230 would be trotted out many times in subsequent cases.

U.S. District Judge Paul L. Friedman wrote in Blumenthal v. Drudge:

The near instantaneous possibilities for the dissemination of information by millions of different information providers around the world to those with access to computers and thus to the Internet have created ever-increasing opportunities for the exchange of information and ideas in “cyberspace.” This information revolution has also presented unprecedented challenges relating to rights of privacy and reputational rights of individuals, to the control of obscene and pornographic materials, and to competition among journalists and news organizations for instant news, rumors and other information that is communicated so quickly that it is too

46. Id.
often unchecked and unverified. Needless to say, the legal rules that will govern this new medium are just beginning to take shape.\textsuperscript{48}

Judge Friedman was correct in his forecast that this burgeoning area of the law would need to be sorted out over time. For his part, Friedman empathized with the Blumenthals, who argued that Drudge was different from an anonymous poster who simply used AOL as a conduit. Indeed, Drudge was paid by AOL and touted by the service.\textsuperscript{49} But in the end, the court noted that Congress intended to provide a wide degree of latitude to ISPs. In so ruling, Judge Friedman observed,

But Congress has made a different policy choice by providing immunity even where the interactive service provider has an active, even aggressive role in making available content prepared by others. In some sort of tacit \textit{quid pro quo} arrangement with the service provider community, Congress has conferred immunity from tort liability as an incentive to Internet service providers to self-police the Internet for obscenity and other offensive material, even where the self-policing is unsuccessful or not even attempted.\textsuperscript{50}

Clearly, Congress recognized the potential of the fledgling medium and did not want to impede its development, finding in the CDA that "[t]hese services offer users a great degree of control over the information that they receive, as well as the potential for even greater control in the future as technology develops."\textsuperscript{51} In carving out immunity for service providers, lawmakers hoped "to preserve the vibrant and competitive free market that presently ex-

\textsuperscript{48} Id. at 49 (footnote omitted).
\textsuperscript{49} Id. at 51 (noting "AOL [promoted] Drudge to its subscribers and potential subscribers as a reason to subscribe to AOL").
\textsuperscript{50} Id. at 52.
ists for the Internet and other interactive computer services, unfea-
tered by Federal or State regulation." 52

In many respects, Congress's plan for the Internet had been validated by the Fourth Circuit Court of Appeals five months be-
before Blumenthal in Zeran v. America Online, Inc. 53

Kenneth Zeran was the subject of an anonymous online prank that caused him massive problems. An unidentified user posted Zeran's name and home telephone number on an AOL bulletin board, offering for sale "shirts featuring offensive and tasteless slogans related to the April 19, 1995, bombing of the Alfred P. Murrah Federal Building in Oklahoma City" 54 and inviting people to call and order. After Zeran experienced a high volume of angry calls, including death threats, he reported the incident to both AOL and law enforcement authorities. 55 To make matters worse, an Oklahoma City radio station obtained a copy of the AOL posting and read it on the air—further urging listeners to inundate Zeran with angry phone calls. 56 Zeran sued AOL, which answered his complaint with a motion for judgment on the pleadings, relying on § 230. The district court agreed with AOL that the CDA provision barred Zeran's claims. 57

The Fourth Circuit also affirmed that Zeran could not pur-
sue claims against AOL because of the federal statute. The court noted that "[t]he specter of tort liability in an area of such prolific speech would have an obvious chilling effect." 58 The unanimous court also found Congress's rationale to be highly transparent, writing:

The purpose of this statutory immunity is not difficult to discern. Congress recognized the threat that tort-based lawsuits pose to freedom

52. Id. § 230(b)(2).
53. 129 F.3d 327 (4th Cir. 1997).
54. Id. at 329 (describing how "[t]hose interested in purchasing the shirts were instructed to call 'Ken' at Zeran's home phone number in Seattle, Washington").
55. Id.
56. Id.
57. Id. at 330.
58. Id. at 331.
of speech in the new and burgeoning Internet medium. The imposition of tort liability on service providers for the communications of others represented, for Congress, simply another form of intrusive government regulation of speech. Section 230 was enacted, in part, to maintain the robust nature of Internet communication and, accordingly, to keep government interference in the medium to a minimum.  

The court also dismissed Zeran’s argument that AOL was put on notice of the posting and thereby lost the immunity granted under § 230. The panel pointed out the flaws inherent in this argument, writing:

More generally, notice-based liability for interactive computer service providers would provide third parties with a no-cost means to create the basis for future lawsuits. Whenever one was displeased with the speech of another party conducted over an interactive computer service, the offended party could simply “notify” the relevant service provider, claiming the information to be legally defamatory. In light of the vast amount of speech communicated through interactive computer services, these notices could produce an impossible burden for service providers, who would be faced with ceaseless choices of suppressing controversial speech or sustaining prohibitive liability.

In Zeran’s case, the online “prank” escalated beyond mere inconvenience to a point where his physical safety was in jeopardy.

59. Id. at 330.
60. Id. at 332.
61. Id. at 333 (suggesting further that “[b]ecause the probable effects of distributor liability on the vigor of Internet speech and on service provider self-regulation are directly contrary to § 230’s statutory purposes, we will not assume that Congress intended to leave liability upon notice intact”).
Still, the courts refused to tamp down the immunity that Congress had set forth for online service providers.

Similarly, even when the online misconduct interferes with the operation of a business, courts traditionally have upheld § 230 protection, despite the problems caused, as the next pair of cases illustrates.

In *Ben Ezra, Weinstein, and Co., Inc. v. America Online, Inc.*, a publicly traded computer finance software manufacturer sued AOL for defamation and negligence for publishing incorrect stock price and share volume information on three occasions. AOL had contracts with ComStock and Townsend, two independent stock quote providers, to supply the financial information AOL posted on its “Quotes & Portfolios service area.”

The plaintiff argued that AOL was not entitled to § 230 immunity because it exceeded the bounds of merely providing online service when it “worked so closely with ComStock and Townsend in the creation and development of the stock quotation information.” That close working relationship amounted to AOL’s notifying the stock quote providers when it learned of incorrect information. The court was not convinced. Writing for a unanimous panel, Circuit Judge Bobby R. Baldock noted, “[w]hile Defendant did communicate with ComStock and Townsend each time errors in the stock information came to its attention, such communications simply do not constitute the development or creation of the stock quotation information.” Moreover, the contract governing the relationship between the stock quote providers and AOL “specifically provided that ‘AOL may not modify, revise, or change’ the information which ComStock provided.”

62. 206 F.3d 980 (10th Cir. 2000).
63. *Id.* at 983.
64. *Id.*
65. *Id.* at 985.
66. *Id.*
67. *Id.* at 986.
II. CRACKS IN THE WALL: HOW SAFE IS SECTION 230'S BLANKET IMMUNITY?

The most recent cases in this area reveal almost complete reliance on § 230 to resolve any dispute in which the ISP is implicated. This raises the question whether mounting pressure—particularly in light of increasingly egregious fact patterns and calls by some legal scholars to revisit the law—eventually will result in congressional action to reduce the blanket safeguard or judicial narrowing of the scope of protection. It is instructive to examine some of the more recent actions to develop a sense of how pivotal the protection is to the conduits of online information, just how far courts have been willing to extend the line between ISP and information content provider, and whether such extension invites criticism and supports advocates seeking to rein in § 230.

In January 2009, a U.S. district court in Texas ruled in favor of the operators of a website called “The Rip-Off Report,” a forum that permitted third parties to voice complaints about companies. GW Equity, a mergers and acquisitions consulting group, sued Xcentric Ventures, claiming the company and its manager “published defamatory reports about [it] on their websites, and developed, wrote, created, edited, and published information contained in the titles and headings of the reports.” The latter point was emphasized by the plaintiff as a means of transforming Xcentric Ventures, for purposes of its lawsuit, from a mere service provider to an information content generator not subject to § 230 protection.

GW Equity argued that content monitors working for Xcentric Ventures “created and developed titles and headings to the published reports regarding [it].” Xcentric Ventures disputed that

68. See, e.g., PALFREY & GASSER, supra note 14, at 106 (arguing that “[t]he scope of the immunity the CDA provides for online service providers is too broad”).
70. Id. at *3.
71. Id. at *4.
allegation, prompting GW Equity to claim summary judgment was inappropriate because a genuine issue as to a material fact existed in the case.\textsuperscript{72} The district court disagreed. Despite testimony before a U.S. magistrate judge in an earlier proceeding that some content monitors added geographical information to the titles of the reports, the district court found such additional content was not enough to establish liability on the part of the ISP.\textsuperscript{73} The court observed:

Thus, even if Plaintiff could prove by a preponderance of the evidence that Defendants added geographical information to the allegedly disparaging titles of the disparaging reports at issue in this case, the Court finds the addition of geographical information alone would not be sufficient for Defendants to be liable for defamation/libel, interference with business relationship, business disparagement under Texas law, disclosure of trade secrets and confidential information, and civil conspiracy as a matter of law.\textsuperscript{74}

To this point, the district court also noted that “[u]nder the CDA, website operators are only considered ‘information content providers,’ for the information at issue that the operators are responsible for creating or developing.”\textsuperscript{75} The court also was in accord with a Fifth Circuit Court of Appeals decision eight months earlier which noted that “[c]ourts have construed immunity under the CDA broadly in all cases arising from the publication of user-generated content.”\textsuperscript{76}

The Fifth Circuit in \textit{Doe v. MySpace}\textsuperscript{77} refused to allow a user of the social networking site to recover damages from the ISP for its alleged failure “to implement basic safety measures to pre-
vent sexual predators from communicating with minors on its Web site.”

“Julie Doe,” thirteen years old at the time, created a MySpace profile, lying about her age and claiming to be eighteen. Because of her misrepresentation, her profile went public, and she was contacted by nineteen-year-old Pete Solis, who subsequently met her in person and sexually assaulted her.

In their action against the ISP, claiming negligence and gross negligence, the plaintiffs argued that § 230 was inapplicable “because their claims do not implicate MySpace as a ‘publisher’ protected by the Act and because MySpace not only published but was also partially responsible for creating the content of the information that was exchanged between Julie and Solis.” With respect to the Does’ argument that their case was “predicated solely on MySpace’s failure to implement basic safety measures to protect minors,” the court of appeals agreed with the district court’s rejection of the claim, noting the lower tribunal’s finding:

The Court, however, finds this artful pleading to be disingenuous. It is quite obvious the underlying basis of Plaintiffs’ claims is that, through postings on MySpace, Pete Solis and Julie Doe met and exchanged personal information which eventually led to an in-person meeting and the sexual assault of Julie Doe. If MySpace had not published communications between Julie Doe and Solis, including personal contact information, Plaintiffs assert they

78. Id. at 416.
79. Id. The court noted:

MySpace.com membership is free to all who agree to the Terms of Use. To establish a profile, users must represent that they are at least fourteen years of age. The profiles of members who are aged fourteen and fifteen are automatically set to ‘private’ by default, in order to limit the amount of personal information that can be seen on the member’s profile by MySpace.com users . . .

Id.
80. Id.
81. Id. at 417.
never would have met and the sexual assault never would have occurred. No matter how artfully Plaintiffs seek to plead their claims, the Court views Plaintiffs' claims as directed toward MySpace in its publishing, editorial, and/or screening capacities. 

The Does' other argument, that MySpace was partially responsible for the content (and thus an information content provider under § 230), was based on the fact “that it facilitates its members' creation of personal profiles and chooses the information they will share with the public through an online questionnaire.” The court of appeals found no basis for such a finding, choosing instead to rely upon the broad swath of protection that courts traditionally have afforded ISPs. The court observed that “[p]arties complaining that they were harmed by a Web site's publication of user-generated content have recourse; they may sue the third-party user who generated the content, but not the interactive computer service that enabled them to publish the content online.” Nevertheless, the remedy of suing the third-party content generator is viable only if that party is identified.

The Does petitioned the Supreme Court for review, but certiorari was denied. In their Reply in Support of Petition for a Writ of Certiorari, the petitioners argued,

This case vividly demonstrates the need for the Court to reign in the overly expansive jurispru-

---

82. Id. at 419-20 (quoting Doe v. MySpace, Inc., 474 F. Supp. 2d 843, 849 (W.D. Tex. 2007)).
83. Id. at 420. The court noted:

The Does also contend that MySpace's search features qualify it as an “information content provider,” as defined in the CDA: “The term ‘information content provider’ means any person or entity that is responsible, in whole or in part, for the creation or development of information provided through the Internet or any other interactive computer service”

Id. (citation omitted).
84. Id. at 419.
dence that has culminated in the Fifth Circuit's finding Section 230 to be a fount of boundless immunity and confirm the correctness of the Seventh Circuit's restrained view, which appropriately respects statutory text, congressional purpose, and state sovereignty. 86

The reference to the Seventh Circuit's treatment of the issue relates to that court's March 2008 decision in Chicago Lawyers' Committee for Civil Rights Under Law, Inc. v. Craigslist, Inc., 87 noted above. 88 Specifically, the Does relied on the court's stated understanding that "Section 230(c) as a whole cannot be understood as a general prohibition of civil liability for web-site operators and other online content hosts." 89 In fact, the Does argued "the truly limited view of Section 230 confines its application to those cases in which the plaintiff brings a claim sounding in defamation that seeks to impose traditional 'publisher' liability on an interactive service provider." 90

A. Beyond Defamation: Immunity for Other Statutory Violations

In Lawyers' Committee, the court of appeals agreed that Congress did not contemplate the fair housing law when it created the immunity under § 230, but noted "the reason a legislature writes a general statute is to avoid any need to traipse through the United States Code and consider all potential sources of liability, one at a time." 91 Parsed differently, the question is not whether Congress meant to include any particular law; rather, the correct question is whether it specifically excluded any act from the law's reach. 92

---

87. 519 F.3d 666 (7th Cir. 2008).
88. See supra note 25 and accompanying text.
89. Lawyers' Committee, 519 F.3d at 669.
91. Lawyers' Committee, 519 F.3d at 671.
92. Id.
A second § 230 case involving the fair housing laws decided in 2008 is distinguishable from Lawyers’ Committee, and the points of distinction are instructive in determining where immunity ends and liability begins. The case perhaps gives some insight into how courts may find ways to assist plaintiffs when an online service aids in violation of a law. For the Ninth Circuit, the issue was not whether § 230 protection applies in anti-discrimination cases. Instead, the question was how responsible the Roommates website was for creating the discriminatory advertisements that appeared on it. The service works by matching “people renting out spare rooms with people looking for a place to live” or, as the court described the operation:

Before subscribers can search listings or post housing opportunities on Roommate’s website, they must create profiles, a process that requires them to answer a series of questions. In addition to requesting basic information—such as name, location and email address—Roommate requires each subscriber to disclose his sex, sexual orientation and whether he would bring children to a household. Each subscriber must also describe his preferences in roommates with respect to the same three criteria: sex, sexual orientation and whether they will bring children to the household.

Chief Judge Alex Kozinski noted that the case would require the court to “plumb the depths of the immunity provided by section 230.” To be clear, the court suggested that a single entity could act as both a content provider and an ISP. The court observed that if the ISP “passively displays content that is created entirely by third parties, then it is only a service provider with respect

93. Fair Hous. Council of San Fernando Valley v. Roommates.com, 521 F.3d 1157 (9th Cir. 2008).
94. Id. at 1161.
95. Id.
96. Id.
97. Id. at 1162.
to that content. But as to content that it creates itself, or is ‘responsible, in whole or in part’ for creating or developing, the website is also a content provider.” 98

When the service provider elicits responses through its online options that give rise to discriminatory (i.e., illegal) content,99 it moves beyond the § 230 protection contemplated by Congress. At that point, it shares the content creation with the users who are choosing among the options provided. The court hastened to point out “the fact that users are information content providers does not preclude Roommate from also being an information content provider by helping ‘develop’ at least ‘in part’ the information in the profiles.”100

Not all First Amendment lawyers were troubled by the court’s decision in Roommates. Speaking to the attendees at the Practising Law Institute’s “Communications Law in the Digital Age” forum in November 2008, Gannett Company, Inc.'s vice president and associate general counsel Barbara W. Wall said “she

98. Id. (quoting Anthony v. Yahoo! Inc., 421 F. Supp. 2d 1256, 1262 (N.D. Cal. 2006)).
99. Id. at 1165. The court noted, for example:
   Roommate requires subscribers to specify, using a drop-down menu provided by Roommate, whether they are “Male” or “Female” and then displays that information on the profile page. Roommate also requires subscribers who are listing available housing to disclose whether there are currently “Straight male(s),” “Gay male(s),” “Straight female(s)” or “Lesbian(s)” living in the dwelling. Subscribers who are seeking housing must make a selection from a drop-down menu, again provided by Roommate, to indicate whether they are willing to live with “Straight or gay” males, only with “Straight” males, only with “Gay” males or with “No males.” Similarly, Roommate requires subscribers listing housing to disclose whether there are “Children present” or “Children not present” and requires housing seekers to say “I will live with children” or “I will not live with children.” Roommate then displays these answers, along with other information, on the subscriber’s profile page.

Id.

100. Id.
is ‘heartened’ by the Roommates.com decision, rather than seeing it as a ‘threat’ to Section 230.” Specifically, she took comfort in the fact that “[a]s distinguished from other cases, by requiring answers to its questions, ‘roommates.com turned your computer into [a Fair Housing Act] violation machine.’” In short, Wall’s comfort level with the decision is based upon the fact that the questions asked by the service would be illegal to ask in other contexts. Thus, it is not a stretch to make it illegal online. Undoubtedly, many First Amendment advocates would concede that plaintiffs have the right to pursue actions against the content generators—provided they can locate them. This gives rise to the burgeoning sidebar to the § 230 story: Can litigants use traditional discovery techniques to locate potential defendants?

III. UNMASKING PUBLIUS: USING SUBPOENAS TO IDENTIFY ANONYMOUS POSTERS

While § 230 shields ISPs from lawsuits arising out of third-party content, clearly the third parties themselves remain fair game for litigation. The recurring problem for plaintiffs is identifying who the message originator is—especially because so much of the speech at issue is anonymous. That fact also raises the specter of the First Amendment because, as one federal court framed the issue, “[t]he right to speak anonymously extends to speech via the Internet. Internet anonymity facilitates the rich, diverse, and far ranging exchange of ideas.”

Indeed, anonymous speech is not a new phenomenon, but the Internet has changed the nature of such communication consid-

102. Id.
104. See, e.g., McIntyre v. Ohio Elections Comm’n, 514 U.S. 334, 342 (1995) (noting that “an author’s decision to remain anonymous, like other decisions concerning omissions or additions to the content of a publication, is an aspect of the freedom of speech protected by the First Amendment”); Talley
erably, given that “[t]he poster’s message not only is transmitted instan-
tantly to other subscribers to the message board, but potentially is
passed on to an expanding network of recipients, as readers may
copy, forward, or print those messages to distribute to others.” 105
With technological advancements also comes the opportunity—
indeed the greater likelihood, given the expansive system—for
more widespread distribution of misinformation, but courts none-
theless often have found that the value of allowing such speech
outweighs the potential for adverse consequences.

The rationale for protecting anonymous speech has been ar-
ticulated by the Supreme Court. In McIntyre v. Ohio Election
Commission, 106 the Court observed,

The decision in favor of anonymity may be mo-
tivated by fear of economic or official retalia-
tion, by concern about social ostracism, or
merely by a desire to preserve as much of one’s
privacy as possible. Whatever the motivation
may be, at least in the field of literary en-
deavor, the interest in having anonymous
works enter the marketplace of ideas unques-
tionably outweighs any public interest in re-
quiring disclosure as a condition of entry. 107

Similarly, other courts have found that anonymous speech
helps to level the playing field for expressive purposes, suggesting
that, “by concealing speakers’ identities, the online forum allows
individuals of any economic, political, or social status to be heard
without suppression or other intervention by the media or more

v. California, 362 U.S. 60, 64 (1960) (suggesting “[a]nonymous pamphlets, leaf-
lets, brochures and even books have played an important role in the progress
of mankind. Persecuted groups and sects from time to time throughout his-
tory have been able to criticize oppressive practices and laws either anony-
mosly or not at all.”).

that “no one is truly anonymous on the Internet, even with the use of a pseu-
donym” because ISPs can trace posters’ identities).

107. Id. at 341-42.
powerful figures in the field.”  

Likewise, in Doe v. Cahill, the Delaware Supreme Court observed,

The internet is a unique democratizing medium unlike anything that has come before. The advent of the internet dramatically changed the nature of public discourse by allowing more and diverse people to engage in public debate. Unlike thirty years ago, when “many citizens [were] barred from meaningful participation in public discourse by financial or status inequalities, and a relatively small number of powerful speakers [could] dominate the marketplace of ideas” the internet now allows anyone with a phone line to “become a town crier with a voice that resonates farther than it could from any soapbox.”

Courts generally have been respectful of the role anonymous speech played throughout history, particularly in establishing the U.S. Constitution, noting specifically that “[t]hroughout the revolutionary and early federal period in American history, anonymous speech and the use of pseudonyms were powerful tools of political debate. The Federalist Papers (authored by Madison, Hamilton, and Jay) were written anonymously under the name ‘Publius.’” Participating in democracy does not require self-identification, and that has a value in itself. “The ‘ability to speak one’s mind’ on the Internet ‘without the burden of the other party knowing all the facts about one’s identity can foster open communication and robust debate.’”

---

108. Krinsky, 72 Cal. Rptr. 3d at 237.
110. Id. at 455 (quoting Lyrissa Narnett Lidsky, Silencing John Doe: Defamation & Discourse in Cyberspace, 49 DUKE L.J. 855, 894 (2000); Reno v. ACLU, 521 U.S. 844, 870 (1997)).
112. Id. (quoting Columbia Ins. Co. v. Seescandy.com, 185 F.R.D. 573, 578 (N.D. Cal. 1999)).
Nonetheless, the question remains: Should a person or entity that is defamed or otherwise injured by an anonymous poster have an opportunity to learn the identity of that poster through the ordinary tools of litigation? Section 230 closes the door, in most instances, on holding the ISP accountable, but should the ISP be forced to cooperate with a subpoena designed with the specific intent of revealing identifying information about the poster? Courts continue to struggle with this issue, and most are treading carefully through this legal thicket, recognizing, as this U.S. district court did, that

[t]he free exchange of ideas on the Internet is driven in large part by the ability of Internet users to communicate anonymously. If Internet users could be stripped of that anonymity by a civil subpoena enforced under the liberal rules of civil discovery, this would have a significant chilling effect on Internet communications and thus on basic First Amendment rights. Therefore, discovery requests seeking to identify anonymous Internet users must be subjected to careful scrutiny by the courts.\textsuperscript{113}

Courts handling the subpoena question could opt for applying standard rules of civil discovery, but this clearly would undermine anonymous speech on the Internet. Instead, requiring a heightened standard when litigants issue a subpoena—clearly the emerging trend—in an attempt to unmask anonymous posters provides a balance of First Amendment interests and helps to ensure

\textsuperscript{113} \textit{Id.} at 1093-94. The court observed:

In the context of a civil subpoena issued pursuant to Fed.R.Civ.P. 45, this Court must determine when and under what circumstances a civil litigant will be permitted to obtain the identity of persons who have exercised their First Amendment right to speak anonymously. There is little in the way of persuasive authority to assist this Court. However, courts that have addressed related issues have used balancing tests to decide when to protect an individual's First Amendment rights.

\textit{Id.}
fairness for parties and potential parties. In *Dendrite International, Inc. v. Doe No. 3*, one of the early cases to address the subpoena issue, the court offered a prescription for handling subpoenas on ISPs seeking the identity of posters:

The trial court must consider and decide those applications by striking a balance between the well-established First Amendment right to speak anonymously, and the right of the plaintiff to protect its proprietary interests and reputation through the assertion of recognizable claims based on the actionable conduct of the anonymous, fictitiously-named defendants. 115

Specifically, the court outlined a four-part approach “based on a meaningful analysis and a proper balancing of the equities and rights at issue.” The four parts of this balancing analysis are as follows:

- The plaintiff must “undertake efforts to notify the anonymous posters that they are the subject of a subpoena or application for an order of disclosure, and withhold action to afford the fictitiously-named defendants a reasonable opportunity to file and serve opposition to the application.” 117

- The plaintiff must “identify and set forth the exact statements purportedly made by each anonymous poster that plaintiff alleges constitutes actionable speech.” 118

- “[T]he plaintiff must produce sufficient evidence supporting each element of its cause of action, on a prima facie basis, prior to a court ordering the disclosure of the identity of the unnamed defendant.” 119

- “[T]he court must balance the defendant’s First Amendment right of anonymous free speech against the strength of the

---

115. Id. at 760.
116. Id. at 761.
117. Id. at 760 (setting out further that “[t]hese notification efforts should include posting a message of notification of the identity discovery request to the anonymous user on the ISP's pertinent message board”).
118. Id.
119. Id.
prima facie case presented and the necessity for the disclosure of the anonymous defendant’s identity to allow the plaintiff to properly proceed.” 120

Other courts have adopted a similar balancing approach. In Doe v. 2TheMart.com Inc., 121 the district court set out the four factors required before ordering the identities of anonymous posters who are not parties to the lawsuit, finding that “non-party disclosure is only appropriate in the exceptional case where the compelling need for the discovery sought outweighs the First Amendment rights of the anonymous speaker”: 122

[T]his Court adopts the following standard for evaluating a civil subpoena that seeks the identity of an anonymous Internet user who is not a party to the underlying litigation. The Court will consider four factors in determining whether the subpoena should issue. These are whether: (1) the subpoena seeking the information was issued in good faith and not for any improper purpose, (2) the information sought relates to a core claim or defense, (3) the identifying information is directly and materially relevant to that claim or defense, and (4) information sufficient to establish or to disprove that claim or defense is unavailable from any other source. 123

In Independent Newspapers, Inc. v. Brodie, 124 Maryland’s case of first impression discussed briefly in the Introduction, the court of appeals explained that it “granted certiorari in this case not merely to sort out the record, but to provide guidance to the trial courts in defamation actions, when the disclosure of the identity of

120. Id. at 760-61 (assuming that “the plaintiff has presented a prima facie cause of action”).
122. Id. at 1095 (observing that “[w]hen the anonymous Internet user is not a party to the case, the litigation can go forward without the disclosure of their identity”).
123. Id.
124. 966 A.2d 432 (Md. 2009).
an anonymous Internet communicant is sought.”¹²⁵ Further, the court “recognize[d] the complexity of the decision to order disclosure regarding pseudonyms or user-names in the context of the First Amendment.”¹²⁶ In the end, however, the state’s high court borrowed from “the standards employed by many of [its] sister courts”¹²⁷ in fashioning Maryland’s five-part rule, which says trial courts “confronted with a defamation action in which anonymous speakers or pseudonyms are involved” should:

(1) require the plaintiff to undertake efforts to notify the anonymous posters that they are the subject of a subpoena or application for an order of disclosure, including posting a message of notification of the identity discovery request on the message board; (2) withhold action to afford the anonymous posters a reasonable opportunity to file and serve opposition to the application; (3) require the plaintiff to identify and set forth the exact statements purportedly made by each anonymous poster, alleged to constitute actionable speech; (4) determine whether the complaint has set forth a prima facie defamation per se or per quod action against the anonymous posters; and (5), if all else is satisfied, balance the anonymous poster’s First Amendment right of free speech against the strength of the prima facie case of defamation presented by the plaintiff and the necessity for disclosure of the anonymous defendant’s identity, prior to ordering disclosure.¹²⁸

Although courts are struggling to establish the appropriate balance in this new area, they recognize that “anonymity or pseu-

¹²⁵. Id. at 449.  
¹²⁶. Id.  
¹²⁷. Id. at 456 (alteration in original).  
¹²⁸. Id. at 457 (citing Dendrite Int’l, Inc. v. Doe No. 3, 775 A.2d 756, 760-61 (N.J. Super. Ct. 2001)).
donymity has been a part of the Internet culture since the outset and preserving those qualities, given the "magnitude of the protection of anonymous speech under the First Amendment," is critical to the future of speech on the Internet.

A. "CyberSLAPPs" as a Threat to Anonymous Speech

The good-faith requirement set out by the district court in Doe v. 2TheMart.com Inc., discussed above, should not be overlooked. Indeed, there is growing concern that some companies are using subpoenas as "weapons" against people who speak out on Internet financial message boards or chat rooms. So called "CyberSLAPPs" attempt to "silence their anonymous critics on the Internet.

129. Id. at 438.
130. Id. at 441.
131. SLAPP stands for Strategic Lawsuits Against Public Participation. For a discussion of SLAPP, see California Anti-SLAPP Project, http://www.casp.net/slapps/mengen.html (last visited Sept. 5, 2009). SLAPPs are:

- civil complaints or counterclaims (against either an individual or an organization) in which the alleged injury was the result of petitioning or free speech activities protected by the First Amendment of the U.S. Constitution. SLAPPs are often brought by corporations, real estate developers, or government officials and entities against individuals who oppose them on public issues. Typically, SLAPPs are based on ordinary civil tort claims such as defamation, conspiracy, and interference with prospective economic advantage. While most SLAPPs are legally meritless, they effectively achieve their principal purpose: to chill public debate on specific issues. Defending a SLAPP requires substantial money, time, and legal resources and thus diverts the defendant's attention away from the public issue. Equally important, however, a SLAPP also sends a message to others: you, too, can be sued if you speak up.

Id. See also CyberSLAPP.org, http://www.cyberslapp.org/ (last visited Sept. 5, 2009). CyberSLAPP.org describes a "CyberSLAPP" as:

involv[ing] a person who has posted anonymous criticisms of a corporation or public figure on the Internet. The target of the criticism then files a frivolous lawsuit just so
boards and intimidate other Internet users to keep their criticisms to themselves.\footnote{Id.} The pattern includes issuing subpoenas against ISPs in an effort to reveal the identities of the anonymous posters, but the impact of the procedural device goes beyond the stated lawsuit: "The free give-and-take of discussion on the boards is also affected. Because users may fear being sued if they criticize the company, they may tone down their criticism or say nothing at all."\footnote{Id. 132. California Anti-SLAPP Project, CyberSLAPPs: Company lawsuits against anonymous Internet posters, http://www.casp.net/slapps/cyberslapp.html (last visited Sept. 5, 2009).}

The good news for targets of CyberSLAPPs, at least in the twenty-nine states that have dealt with the issue by either statute or case law,\footnote{Id. 133. Id. 134. See California Anti-SLAPP Project, Other States: Statutes and Cases, http://casp.net.statutes/menstate.html (last visited Sept. 5, 2009) (noting the states with anti-SLAPP statutes are: Arizona, Arkansas, California, Delaware, Florida, Georgia, Hawaii, Illinois, Indiana, Louisiana, Maine, Maryland, Massachusetts, Minnesota, Missouri, Nebraska, Nevada, New Mexico, New York, Oklahoma, Oregon, Pennsylvania, Rhode Island, Tennessee, Utah, Vermont, and Washington, while Colorado and West Virginia have created protections through case law). 135. See, e.g., CAL. CIV. PROC. CODE § 425.16 (providing for a claim "arising from 'act in furtherance of a person's right of petition or free speech under the United States or California Constitution in connection with a public issue")}. is that they can defend the lawsuit under their state's anti-SLAPP law. These measures are typically designed to bring about a quick disposition of the case believed to be a SLAPP, immunize the comments of the citizens who have spoken out and allow for attorneys fees and costs if the court determines that the lawsuit was filed for a nefarious purpose (i.e., to retaliate against someone or shut off discussion in a community).\footnote{Id. § 425.16(g).} Importantly, these laws often require that discovery be stayed while the court considers the early motions to strike the lawsuit.\footnote{Id. 136. Id. § 425.16(g).}

---

Id.


133. Id.


135. See, e.g., CAL. CIV. PROC. CODE § 425.16 (providing for a claim "arising from 'act in furtherance of a person's right of petition or free speech under the United States or California Constitution in connection with a public issue")

136. Id. § 425.16(g).
Amid rising concerns about potential CyberSLAPPs, California took the bold defensive step of enacting protections against subpoenas for "personally identifying information" when the underlying lawsuit involves the exercise of free speech rights.\footnote{CAL. CIV. PROC. CODE § 1987.1(b)(5) (noting that "[a] person whose personally identifying information . . . is sought in connection with an underlying action involving that person's exercise of free speech rights" may seek a protective order from a court. The law went into effect Jan. 1, 2009.).} California Assembly member Paul Krekorian, the primary sponsor of the measure, noted in a press release that CyberSLAPPs require special attention: "As greater numbers of Californians are turning to the Internet to speak out on controversial issues, their freedom to express themselves anonymously must be protected from powerful parties who threaten and use oppressive litigation tactics to stifle criticism and dissenting views."\footnote{Press Release, Assistant Majority Leader Paul Krekorian, Krekorian Bill to Protect Freedom of Speech on the Internet Passes Senate Comm. (July 2, 2008), http://democrats.assembly.ca.gov/members/a43/News_Room/press/20080702AD43PR02.aspx.}

When California Governor Arnold Schwarzenegger signed the bill into law in October 2008, the Electronic Frontier Foundation\footnote{See Electronic Frontier Foundation, http://www.eff.org/about (last visited Sept. 5, 2009) (describing how "EFF broke new ground when it was founded in 1990—well before the Internet was on most people's radar—and continues to confront cutting-edge issues defending free speech, privacy, innovation, and consumer rights today").} observed on its "Deeplinks Blog" that:

\begin{quote}
[O]ne of the most pernicious threats to anonymity is the filing of trumped-up lawsuits as an excuse to force ISPs to reveal speakers' identities. Once such a lawsuit is filed, speakers who want to protect their anonymity must find a way to pay a lawyer to go to court and prevent disclosure of their personal information. That can be a real hardship—in fact, even the threat of having to go to court may discourage many people from speaking out in the first place.\footnote{Posting of Corynne McSherry to Deeplinks Blog, California Governor Signs Off On New Protections for Free Speech,}.
\end{quote}
California was a leader in enacting anti-SLAPP laws in the early 1990s, so it's not surprising that the state would be out front in fighting the next iteration of these lawsuits that pose a serious threat to free speech.\footnote{141}

B. Shielding Bloggers under Journalistic Privilege Laws

While California law protects against subpoenas in Cyber-SLAPP cases to reveal the identity of critics, newspapers that host blogs now have another tool in combating similar “fishing expeditions”: shield laws.\footnote{142} Statutes shielding journalists from having to disclose information in official proceedings—now found in thirty-six states\footnote{143}—“vary, often substantially, from state to state.”\footnote{144} Nonetheless, the use of shield laws to keep confidential the identity of anonymous posters to newspaper blogs, though a novel and nascent concept, was allowed by trial courts in at least three states in 2008.

In October 2008, the Circuit Court in Okaloosa County, Florida, ruled that the Florida Shield Law\footnote{145} protected the records custodian/webmaster at the \textit{Florida Freedom}, a daily newspaper serving the area, from having “to appear and produce information

\footnote{141. See Richards, supra note 24, at 20 (describing the early process of passing anti-SLAPP legislation in California).}

\footnote{142. See Don R. Pember & Clay Calvert, Mass Media Law 637 (2009-2010 ed. 2008) (describing shield laws as “[s]tate statutes that permit reporters in some circumstances to shield the name of a confidential news source when questioned by a grand jury or in another legal forum”).}


\footnote{144. C. Thomas Dienes et al., News Gathering and the Law 969 (1998) (noting that “[s]ome statutes extend their protections to those persons ‘engaged in newspaper, radio or television journalism,’ while others apply to any person ‘regularly engaged in the business of collecting or writing news for publication, or presentation to the public, through a news organization’”) (citations omitted).}

and records related to an Internet poster to Florida Freedom's website including, but, not limited to, the user's e-mail and IP addresses and other identifying information.\textsuperscript{146}

In quashing the subpoena, the court noted that the webmaster "was at all material times a professional journalist employed by" the newspaper.\textsuperscript{147} Under Florida's statute, a "[p]rofessional journalist" is someone who regularly "engage[s] in collecting, photographing, recording, writing, editing, reporting, or publishing news, for gain or livelihood, who obtained the information sought while working as a salaried employee of, or independent contractor for, a newspaper, news journal, news agency, press association, wire service, radio or television station, network, or news magazine."\textsuperscript{148}

Interestingly, the privilege extends to "information, including the identity of any source, that the professional journalist has obtained while actively gathering news."\textsuperscript{149} Accordingly, for the court to stretch the privilege to cover the situation where an anonymous website visitor posts to a newspaper's blog, it had to find that the definition of newsgathering sweeps up the unchecked postings of third parties. Stated differently, by posting to a newspaper's blog rather than other available sites, a third-party poster may receive a layer of protection under a statute that originally was designed to protect journalists who rely upon confidential sources in the process of reporting the news. Moreover, the court applied the test that a party must show to overcome the privilege and found that the individual seeking the identity of the Internet poster "failed to meet the burden."\textsuperscript{150}

\textsuperscript{146} Beal v. Calobrisi, No. 08-CA-1075, slip op. at 2 (Fla. Cir. Ct. Oct. 9, 2008).
\textsuperscript{147} Id.
\textsuperscript{148} FLA. STAT. ANN. § 90.5015 (a).
\textsuperscript{149} Id. § 90.5015(2) (emphasis added).
\textsuperscript{150} Beal at 2. The test requires a three-part showing to overcome the privilege: "(a) The information is relevant and material to unresolved issues that have been raised in the proceeding for which the information is sought; (b) The information cannot be obtained from alternative sources; and (c) A compelling interest exists for requiring disclosure of the information." § 90.5015(2).
Similarly, in Oregon, Clackamas County Circuit Court Judge Pro Tem James E. Redman ruled that "[t]he Oregon Media Shield Law is broadly written and it is intended to protect a broad range of media activity, not simply news gathering." The plaintiff sought to compel "the production of information helpful to identify the authors of anonymous web blog comments" from two web hosts, Willamette Week and Portland Mercury. The judge found that both hosts fell "within the purview" of Oregon’s shield law, which applies to persons "connected with, employed by or engaged in any medium of communication to the public."

The judge used the portion of the statute that protected "[t]he source of any published or unpublished information obtained by the person in the course of gathering, receiving or processing information for any medium of communication to the public." The court noted that the plaintiff would have the court read the language "in the course of gathering . . . information" to be "synonymous with 'in the course of gathering news'" and thus not applicable to the anonymous posting scenario. Judge Redman declined to read the statute that narrowly, saying that "[i]t would seem clear that Oregon’s Media Shield Law is intended to have a wider scope than 'news gathering.'"

When news organizations host blogs, they often do so in conjunction with their own reporting. A post on the Portland Mercury’s blog entitled “Busy Day at City Hall, Part 2” discussed a mayoral candidate’s actions to secure public financing for his campaign and invited readers to post comments on the blog. An

152. Id.
153. Id.; OR. REV. STAT. § 44.520 (2007).
154. OR. REV. STAT. § 44.520(1)(a).
156. Id.
anonymous poster named “Ronald” responded with a comment that was allegedly defamatory.\(^{158}\)

The court microparsed the shield law’s protection, finding that if “the comment had been totally unrelated to the blog post, then the argument could be made that the Portland Mercury did not receive it in the ‘course of gathering, receiving, or processing information for any medium of communication to the public.’”\(^{159}\)

Under the circumstances, however, the statute applied.

In a third case, in Montana, a one-time politician tried to force the Billings Gazette to turn over identifying information about posters to the newspaper’s blog who used the pseudonyms “Always Wondering,” “High Plains Drifter,” and “CutiePie.”\(^{160}\) As in the cases discussed above, the newspaper sought protection from the subpoena under Montana’s shield law, known as the “Media Confidentiality Act.”\(^{161}\) The language of Montana’s shield law has a broad sweep and states that no one who is involved in “gathering, writing, editing, or disseminating news may be examined as to or may be required to disclose any information obtained or prepared or the source of that information in any legal proceeding if the information was gathered, received, or processed in the course of his employment or its business.”\(^{162}\)

The Billings Gazette argued, in moving to quash the subpoena, “that the on-line message service is indeed part of the Gazette’s business . . . an integral part of the business and a growing part of the business.”\(^{163}\)

Judge G. Todd Baugh agreed that the statute is expansive enough to encompass anonymous posters to the newspaper’s website. In ruling from the bench, he noted that:

\(^{158}\) See Letter from James E. Redman, supra note 151, at 2.

\(^{159}\) Id. (noting that “[t]his court feels compelled to follow the broad statutory language in regard to plaintiff’s motion to compel and therefore denies plaintiff’s motion to compel”).

\(^{160}\) Transcript of Motion to Quash at 11, Doty v. Molnar, Cause No. DV 07-022 (Mont. 13th Jud. Dist. Sept. 3, 2008) (on file with author).

\(^{161}\) MONT. CODE ANN. § 26-1-901 (2007).

\(^{162}\) Id. § 26-1-902(1).

\(^{163}\) Transcript of Motion to Quash, supra note 160, at 4 (on file with author).
the Court doesn't even get to the constitutional issue that the legislature has already decided . . . with this statute. And though technology has advanced since the time of the creation of that law, it, nonetheless, is very broad and it does cover the situation we have here before us today.¹⁶⁴

While the use of shield law protections to avoid unmasking anonymous posters to a media organization's blog is a recent phenomenon, it has captured the attention of media lawyers and thus promises to grow in popularity. The respected media law firm of Levine Sullivan Koch & Schulz, L.L.P.¹⁶⁵ reported on the practice in a recent newsletter to clients and other interested parties in an update article entitled, "How to Respond to Subpoenas Seeking to Unmask Anonymous Internet Posters."¹⁶⁶ In informing clients about how subpoenas may be challenged, the article observed that "[u]nder certain circumstances, media companies can challenge a subpoena seeking identifying information. For example, companies might ask a court to quash a subpoena based on the speaker's constitutional rights, federal and state statutory law, the reporter's privilege, or the court's lack of jurisdiction."¹⁶⁷

IV. ANALYSIS

BALANCING FIRST AMENDMENT INTERESTS AND PERSONAL HARM IN THE AGE OF THE INTERNET: A PROPOSED LEGISLATIVE SOLUTION

Unquestionably, the law regarding the insulation of ISPs from lawsuits stemming from third-party content is a work in progress. The latest trends indicate that the standard discovery tool for

¹⁶⁴. Id. at 29.
¹⁶⁷. Id. (emphasis added).
compelling ISPs to turn over identifying information about the third-party poster—the subpoena—presents ancillary (yet critical) issues that may undermine long-established free speech principles, such as the right to speak anonymously. On the other hand, the ability to disseminate potentially damaging and false information about another to a mass audience with little more than a keystroke’s worth of effort threatens to devalue reputation to a point never before experienced in American culture.

The question then becomes: is there a way to balance the First Amendment rights of ISPs and posters with the reputational interests of those who allegedly are harmed by the online material? Any such balancing would require a revision of the blanket immunity under § 230 and thus portends a statutory solution. Necessarily, any such congressional action must contemplate choices that would be freely elected by the parties involved. What follows is a proposed template for achieving that balance while maintaining, to the fullest extent possible, the First Amendment safeguards for online speech. It maps out a process for handling a variety of situations that often arise with online postings.

At the outset, it is important to point out that no section of the proposed solution outlined below imposes an affirmative obligation on the ISP to police content on its site—an unduly burdensome, if not crippling, task. Any requirement forcing the ISP to act would be triggered only by the individual alleging harm arising out of the information posted on the site—with appropriate safeguards against frivolous claims and likely “fishing expeditions.”

A. Status Quo: The Identity of the Poster is Readily Available

In situations in which the identity of the online poster is apparent, the only recourse for the aggrieved party is to file a lawsuit—if an actionable claim exists—against the third-party content provider. Section 230 insulation from claims, under such circumstances, would remain firmly in place for the ISP.
B. Anonymous Posters: Identifying Information Available Only to Internet Service Provider

If the posting at issue comes from a third-party who has posted anonymously or by using a pseudonym, then the aggrieved party has the affirmative obligation to contact the ISP and provide notice of the exact posting(s) that give rise to legally actionable material (defamation, privacy, or other violations of law). Once notified of legally actionable material, the ISP has several choices—each of which would affix certain liabilities, rights, and responsibilities.

i. Refusal to Act

The first choice for the ISP is simply to do nothing. If the ISP chooses this option, the immunity currently available under § 230 may dissolve and the ISP could be subject to legal action as if it were the provider of the content at issue. Nonetheless, even under such circumstances, the ISP would still have all of the usual defenses that any publisher of information would have available to it under federal and state constitutions, statutory, and common law.

Additional protection is warranted. Thus, if it is determined that the legal action taken against the ISP and poster (if eventually identified and added to the lawsuit) was not carried out in good faith (i.e., there is no legitimate cause of action or the action was initiated for sham purposes), the ISP would be entitled to an expedited disposition of the case (e.g., a motion to strike staying discovery) and reasonable attorneys' fees and costs, similar to the way anti-SLAPP laws operate in the states that have enacted them. Accordingly, an ISP that correctly believes the material in question is protected speech can defend a lawsuit without fear of burdensome costs.

ii. Process to Retain Insulation Against Legal Action

To retain for itself the immunity currently available under § 230, the ISP must contact the unidentified poster and offer the opportunity to remove the posting within a statutorily defined period
of time (say, ten days).\textsuperscript{168} If the poster consents to removal, or if the ISP decides to do so on its own, immunity attaches to the ISP, and no cause of action may follow against it.

Moreover, if the poster refuses removal, and the ISP does not do so on its own, but cooperates fully with any subpoena or order of court to reveal identifying information available to it about the poster, the ISP will be immune from any liability.

iii. Piercing the “Virtual” Veil

If the poster does not consent to removal and the ISP does not remove the content on its own, then the aggrieved party may proceed against both the ISP and the unidentified poster as a “Doe” defendant. If the aggrieved party issues a subpoena or a court orders disclosure and the ISP challenges such disclosure,\textsuperscript{169} then the case proceeds against both the ISP and the poster. In this situation, the traditional defenses against the cause(s) of action will come into play. Moreover, as in the case in which the ISP does nothing, if it is shown that the plaintiff did not act in good faith in pursuing the lawsuit, reasonable attorneys’ fees and costs are available to the ISP. Insofar as the subpoena challenge is concerned, Congress should codify a version of the tests set forth by the several courts that examined this issue. In all such cases, the ISP should take reasonable steps to notify the poster that a subpoena has been issued in order that the poster be afforded the opportunity to chal-

\textsuperscript{168} Some legal commentators have proposed “notice and takedown” provisions similar to those found in the Digital Millenium Copyright Act, 17 U.S.C. §§ 512(c) & 512(d) (2006). See Olivera Medenica & Kaiser Wahab, Does Liability Enhance Credibility?: Lessons from the DMCA Applied to Online Defamation, 25 CARDOZO ARTS & ENT. L.J. 237, 265 (2007) (proposing an “Online Defamation Limited Liability Act” in which “once an ISP receives written notice of an allegedly defamatory statement pursuant to a statutory notice requirement, the ISP would have to take down the defamatory materials for a finite period of time, such as ten to fourteen days”). This differs considerably from the proposal herein, in that in the current proposal, any such takedown by the ISP is voluntary. Moreover, the scope of the current proposal moves beyond simple defamation cases.

\textsuperscript{169} As suggested earlier, if the ISP cooperates and reveals identifying information, immunity attaches to the ISP.
lenge the subpoena. The ISP would have that same opportunity. The following hybrid of the judicially-created tests, which establish a heightened standard, would serve to balance the interests of the parties:

- The court must examine the statements at issue in the complaint to see if there is a prima facie showing that a violation of law exists. Clearly, this determination relates to the good-faith requirement outlined above.
- The court must be satisfied that the information sought by the subpoena is necessary to prove a core claim or defense in the case.
- The information sought is not available from any other source.

The full range of privileges currently available in the law—reporter's privilege included—would remain available where applicable.

CONCLUSION

It is no stretch to argue that Congress never envisioned the full range of messages to which § 230 has applied for more than a dozen years. It is also not surprising that given the proliferation of blogs and social networking sites—the seemingly countless opportunities to post damaging information online anonymously—there have been calls for reforms and frustration with the current system that affords little opportunity for those claiming legitimate harms from online messages. Nonetheless, to scrap ISP immunity altogether would be a devastating move that would undermine the usefulness and future growth of the Internet. Moreover, blithely allowing the revelation of anonymous online posters' identities would undercut a tradition of free speech in this country that dates back to the nation's founding.

The only reasonable way to address the situation is to modify the existing law in such a way as to require a heightened standard on the part of those seeking redress, yet leave open the oppor-

170. See supra notes 142–167 and accompanying text (discussing a shield for bloggers under laws that grant privileges to journalists).
tunity for recourse in situations where complainants meet that high threshold. The proposal outlined above allows for potential liability against the ISP only in the situation where an actual cause of action exists against the unidentified poster and the ISP has refused to act in any way.