

REEXAMINING SECTION 230 OF THE CDA AND ONLINE ANONYMOUS
SPEECH: DEFAMATION ON THE INTERNET AND THE WEBSITES THAT
FACILITATE IT

by

Madeleine K. Rodriguez

An honors thesis submitted to the
Department of Communication
of Boston College

Thesis Adviser:
Dr. Dale A. Herbeck

May 2009

Copyright by
MADELEINE K. RODRIGUEZ
2009
All Rights Reserved

To my parents,
for their unwavering support, love, and understanding.

To Dr. Herbeck,
for his patience and good sense of humor.

TABLE OF CONTENTS

CHAPTER ONE: THE COMMUNICATIONS DECENCY ACT	1
Section 230 of the CDA	6
A Prelude to Section 230	6
The Cyberporn Panic of 1995	12
<i>Zeran v. AOL</i>	17
The <i>Zeran</i> Line	24
Internet Content Providers	24
Internet Content Facilitators	29
The Roommates Exception	33
Extending Beyond Defamation	37
CHAPTER TWO: THE INADEQUACIES OF SECTION 230	43
Criticisms of Section 230	46
Congressional Intent	46
Public Policy Argument	54
Double Standard	63
Proposed Solutions	70
Establish Levels of Control	71
Impose Notice and Take Down Requirements	77
Repeal Section 230	83
CHAPTER THREE: A RESPONSE TO THE SECTION 230 DEBATE	88
Answering the Proposed Solutions	89
Establishing Control Levels is Unworkable	89
Notice and Take Down Requirements Are Flawed	93
In Defense of Section 230	102
Social Changes	107
Self-Regulation Standards as a Compromise	114
Features Internet Content Facilitators Should Develop	116
Policy Ideas	121
Conclusion	127

CHAPTER ONE:
THE COMMUNICATIONS DECENCY ACT

“C’mon. Give us the juice”—these were the instructions listed at the top of one of 2008’s most controversial websites, JuicyCampus.com. Created in August 2007 by Duke University graduate Matt Ivestor, the website encouraged students from over 500 college campuses to gossip, rant, and out each other’s most personal secrets.¹ Juicy Campus allowed anyone with a computer to find out which sorority at the University of Florida ranked in the lowest tier or whether or not Ryan Murphy from Princeton liked guys or girls or both. It all seemed like harmless and maybe even insignificant banter when it was given a casual glance, but both the media and students from all over the nation spoke out passionately in favor of the website’s demise. All of this attention, however, left some confused as to why such a fuss was necessary and others wondered who could actually care about the Internet ramblings of college students.

Well, for one, students in Ryan Murphy’s situation cared, and some employers took a look at the site’s content, as well. More and more students found that damaging and false information was being posted on the website for their classmates to view and discuss in detail. Even worse, most people who visited the Juicy Campus website were encouraged by the site owner’s promise that “Posts are totally, 100% anonymous” and

¹ Juicy Campus, “About Us,” <http://juicycampus.com/posts/about-us> (accessed January 23, 2009).

would remain so unless proper court documents were provided.² Obtaining these legal documents is usually easier said than done and certainly does not come cheap. In order to prove that defamation has occurred, those filing a suit must prove that the message in question (1) can be perceived as harmful or insulting; (2) has been heard, read or viewed by a third party; (3) clearly identifies the person being defamed; and (4) demonstrates actual malice or negligence depending on the individuals status as a public or private figure.³ Students pursuing such legal action against their defamers run into a brick wall when the statement in question turns out to be an opinion rather than something that seems like an author is trying to pass off as factual (because everyone's entitled to an opinion). If Ryan Murphy was a star athlete or the president of his university's student government, he also might run into some trouble if the court concluded he is a public figure on his campus, requiring him to prove that the message was posted with actual malice rather than simple negligence.

Regardless of these defamation law principles, however, one thing is absolutely certain—Ryan Murphy can not sue Juicy Campus (or any website like it) for damages. Due to Section 230 of the Communications Decency Act (CDA), Matt Ivestor and his Juicy Campus team are immune from any kind of liability related to the postings on their website, and also have no obligation to remove those postings if a person should complain to their site. What started out as provision which would protect traditional

² Juicy Campus, "Privacy & Tracking Policy," <http://juicycampus.com/posts/privacy-policy> (accessed January 23, 2009).

³ Thomas L. Tedford and Dale A. Herbeck, *Freedom of Speech in the United States*, 5th ed. (State College, Pa: Strata, 2005), 82-83.

Internet service providers (ISPs) like America Online and CompuServe has been interpreted by federal courts to include Internet content providers (ICPs) ranging from retailers such as Amazon.com to online dating websites such as Matchmaker.com. Since an individual or company has never been successful in proving any ISP or ICP liable for disseminating third-party defamatory statements, it is likely that these new types of websites which Juicy Campus represents, probably best labeled as Internet content facilitators (ICFs), will also be granted the same kind of unwavering protection. Many have criticized Section 230 with hopes that it would be amended or thrown out since its inception, and these ICFs have only assured them that this is the best solution to the problems these sites present. Others, including Matt Ivestor, claim that the promotion of free expression on the Internet is far more important than addressing the grievances of a few individuals, and visitors to these types of sites should simply exercise responsibility when choosing their words and remain responsible when those words turn foul.

On February 5, 2009, the Juicy Campus website shut down due to lack of revenue, yet this does not mean that the online defamation issue has also been put to rest. As of March 2009, visiting JuicyCampus.com automatically redirects a visitor to CollegeACB.com (“College Anonymous Confession Board”), a website which provides the same services and functions for the college and university online community that Juicy Campus pioneered.⁴ Likewise, while Juicy Campus garnered most of the attention and negative press, it was only one in a long series of similar websites which provide

⁴ Carrie Thornton, “New Gossip Web Sites Follow in Wake of JuicyCampus.com,” *The Daily Toreador*, March 6, 2009.

forums for individuals to “anonymously” comment on their peers.⁵ If your neighbor is an insufferable human being, RottenNeighbor.com may just be the right outlet for you to vent your frustrations. Finding out your boyfriend cheated on you multiple times may not be as painful an experience when you can run to DontDateHimGirl.com and instruct all of its viewers to never give him the time of day. Other sites tackle teachers (RateMyTeachers.com), professors (RateMyProfessors.com), roommates (Roommates.com), and law school students (AutoAdmit.com) all to the same humiliating and vicious degree. So while Juicy Campus was not the first, its notoriety shined a spotlight on a new wave of websites which allow and facilitate this type of free flowing anonymous speech. Although many continue to fly under the radar which mainly focused on Juicy Campus and its affect on college students, all of these websites have contributed to their own respective controversies and dilemmas for their users and the people they choose to talk about.

Since it is so difficult for defamed parties to deal with these users directly, some individuals have attempted to sue the website itself in hopes that information posted about them can be removed and they can be properly compensated for invasions of their private life and the damage done to their respective reputations. Defamation victims have

⁵ See Jessica Bennett, “What You Don’t Know Can Hurt You,” *Newsweek*, December 17, 2007, Periscope; Marc Fisher, “Dorm Gossip Turns Slimy on the Internet,” *The Washington Post*, March 2, 2008, Section C; Neil Johnson, “Sour Juice,” *The Heights, Independent Student Newspaper of Boston College*, April 4, 2008, Features; Heather Robinson, “On JuicyCampus, Anonymous Posts Pick Yale Apart,” *Yale Daily News*, February 11, 2008.

suggested that, since these websites thrive and essentially encourage this type of behavior, they should bear some responsibility for the defamatory content. As mentioned previously, however, Section 230 has made suing such websites virtually impossible. Since they are merely distributors of information which others create, these websites are immune from liability and have no responsibility to screen or remove the offending message without a court order instructing them to do so.⁶

Due to the difficulties that defamed parties obviously encounter when they attempt to have content removed or recover damages, Section 230 has been widely criticized, and several solutions have been proposed which would make its language more clear and provide affected parties with better avenues to address their grievances. While a clear understanding of the history of Section 230, related cases, and its critics is valuable, a completely new approach may be required when dealing with these new Internet content facilitators. The remaining pages of this chapter introduce the origins of Section 230—how and why it was created and the individual cases that directly impacted this body of law in its early stages. Having laid a foundation, the chapter continues to review some of the most famous cases related to the often anonymous posting of illegal materials on the Internet. As the case history is dissected, it will become increasingly apparent that the courts have interpreted Section 230 to grant immunity to companies or websites which provide service, service and content, facilitate content, or even fall outside the realm of defamation altogether.

⁶ Juicy Campus, “Privacy & Tracking Policy,”

<http://www.juicycampus.com/posts/privacy-policy> (accessed January 23, 2009).

Section 230 of the CDA

A Prelude to Section 230

Back in the 1980s when the Internet was first starting to find its way into the market, CompuServe, was the first online service provider to really get a hold of this commercial industry. If an individual subscribed to their services, which at the time could cost almost thirty dollars an hour, they were promised access to news, weather, encyclopedias, and thousands of other information sources. There were also about 150 special interest forums that CompuServe provided access to, which allowed users to communicate with each other in real time. One of these was a journalism forum which featured a publication known as “Rumorville.” “Rumorville” was created by Don Fitzpatrick Associates and offered to CompuServe subscribers. At the same time, “Skuttlebut,” a competitor created by Robert Blanchard and Cubby, Inc., began reporting similar gossip and news to its readers. In April 1990, the writers of “Rumorville” alerted their readers that the information provided by “Skuttlebut” had mostly been originally published in “Rumorville,” and the “Skuttlebut” team was acquiring this information “through some back door.” This edition of “Rumorville” also personally attacked Blanchard and alleged that he had been “bounced” from his previous job and was obviously attempting to run “a new start-up scam.” After reading these claims which they knew to be false, Cubby and Blanchard sued CompuServe for defamation.⁷

⁷ Summary derived from *Cubby v. CompuServe*, 776 F. Supp. 135 (S.D. N.Y. 1991).

CompuServe, believing that there was “no genuine issue as to any material fact and that [they were] entitled to a judgment as a matter of law,” moved for summary judgment.⁸ Their motion was based on the fact that they considered themselves to be distributors of the information on “Rumorville” and not publishers of its content. This would prove to be a crucial distinction. On one hand, distributors (such as a book store like Barnes and Noble) have no prior knowledge, content control, or editorial control over the messages, products, or forms of expression which they sell or offer as services. The thought is that since distributors have so much content that they handle (Barnes and Noble has thousands of titles, DVDs, CDs, and other products), it is not feasible for them to monitor all of it and screen for defamatory content. A publisher (like Random House), on the other hand, deals with a much more limited set of information which they can plausibly screen before it reaches the masses. Their business model relies on having employees or staff members who review the information beforehand and edit its content as necessary. For these reasons, an individual could reasonably sue a publisher for defamation.

District Judge Peter Leisure of the Southern District of New York now had an important decision to make. CompuServe argued that it was merely a distributor of the information found in “Rumorville” and as such had no prior knowledge as to the defamatory statements being made in its contents. Cubby countered that CompuServe was actually a publisher of these defamatory statements, a publisher which had complete control and knowledge regarding the information available on its network and therefore

⁸ 776 F. Supp. 135, 138 (S.D. N.Y. 1991).

should be “[held] to a higher standard of liability.”⁹ Given that legally, publishers could be held responsible for defamation and distributors could not (due to the belief that publishers could reasonably have prior knowledge, exert content and editorial control, and screen their products and distributors could not), it is fair to conclude that the case rested on this very issue.

In the end, Judge Leisure decided that CompuServe was a distributor and could not be held liable for the defamatory content posted on “Rummorville.” “New York courts,” he explained, “have long held that vendors and distributors of defamatory publications are not liable if they neither know nor have reason to know of the defamation.”¹⁰ CompuServe, he concluded, did not have any prior knowledge of the postings on “Rumorville,” and Judge Leisure felt that expecting distributors to keep a vigilant eye on all such content would be an unreasonable burden. Likening CompuServe to a book distributor, he wrote, “Every bookseller would be placed under an obligation to make himself aware of the contents of every book in his shop. It would be altogether unreasonable...and the bookseller’s burden would become the public’s burden.”¹¹ This marked the first time that the issue of liability on the Internet was formally and explicitly discussed in a legal setting.

A few years later, Prodigy emerged as a “family oriented” computer network with a few million registered users. Prodigy routinely screened for “objectionable” material and maintained a set of guidelines for its users who wished to post content. One of

⁹ 776 F. Supp. 135, 138 (S.D. N.Y. 1991).

¹⁰ 776 F. Supp. 135, 138 (S.D. N.Y. 1991).

¹¹ 776 F. Supp. 135, 139-140 (S.D. N.Y. 1991).

Prodigy's message boards, "Money Talk," was extremely popular, and it contained the most widely read information and opinions regarding stocks, investments, company practices, and other financial and business related topics in the nation. Like all of Prodigy's message boards, "Money Talk" had users who served as discussion leaders and had been contracted by Prodigy to contribute their own content and monitor usage of the boards.

Founded by Jordan Belfort and Danny Porush, Stratton Oakmont was a "pump and dump" brokerage house built on Long Island in the state of New York in the 1990s. When "Money Talk" users began to discuss Stratton Oakmont's practices regarding the public offering of stock of Solomon Page, Ltd, the results were less than complimentary. Several posts alleged that Stratton Oakmont had engaged in criminal and fraudulent acts while advising their clients in regards to this particular stock. More specifically, the "Money Talk" community had members who felt that Danny Porush, the President of Stratton Oakmont at the time, was bound to be charged for criminal activity and that the entire firm was full of brokers who had been indoctrinated into a cult atmosphere that required them to illegally lie and trick their clients in order to remain employed. Unlike the "Rumorville" publication, all of these posts qualified as truly anonymous speech. When Stratton Oakmont learned that such claims were being made on such a well known online source, Stratton Oakmont sued Prodigy for defamation. Using the *Cubby* decision as the basis of their claim, Prodigy similarly moved for summary judgment.¹²

¹² Summary derived from *Stratton Oakmont v. Prodigy*, 23 Media L. Rep. 1794 (N.Y.S. 1995).

This time, however, New York State Judge Stuart Ainsworth denied the computer network's motion on the grounds that it did not function the way CompuServe did. Prodigy made it clear that they claimed editorial control over the content of messages posted on their boards. Judge Ainsworth believed this likened Prodigy to a newspaper and quoted Prodigy's Director of Market Programs and Communications' own words from an article he had written which stated:

We make no apology for pursuing a value system that reflects the culture of millions of American families we aspire to serve. Certainly no responsible newspaper does less when it carries the type of advertising it published, the letters it prints, the degree of nudity and unsupported gossip its editors tolerate.¹³

Additionally, Prodigy regulated their content. They had a set of "content guidelines" for users which dictated what kind of information was acceptable for publication over their network. They used a software screening program which checked every post for offensive language prior to it being published and flagged posts with content they had outlined as objectionable. Prodigy also hired board leaders who facilitated and watched the activity on the boards, and these board leaders also had an emergency delete button at their disposal which they were allowed and instructed to use if an egregious violation of Prodigy's terms ever occurred in online discussions. All of these features gave Prodigy a considerable amount of prior knowledge and control over what was officially published online.¹⁴

¹³ 23 Media L. Rep. 1794, 4 (N.Y.S. 1995).

¹⁴ 23 Media L. Rep. 1794, 5-6 (N.Y.S. 1995).

Judge Ain concluded that Prodigy was not like CompuServe and should, in fact, be considered a publisher rather than a distributor. Citing the features described previously, Judge Ain wrote that Prodigy was “clearly making decisions as to content, and such decisions constitute editorial control.”¹⁵ “Prodigy,” he elaborated, “has uniquely arrogated to itself the role of determining what is proper for its members to post and read on its bulletin boards. Based on the foregoing...Prodigy is a publisher rather than a distributor.”¹⁶ The judge denied the motion for summary judgment, and the case was scheduled for trial on Stratton Oakmont’s defamation claim.

After the summary judgment was denied, the suit was set for court with Stratton Oakmont seeking millions in damages. Instead of going to trial and risking a loss, Prodigy issued a public apology and the suit was dropped. Although this issue ended up disappearing peacefully, the *Stratton Oakmont* decision presented a new predicament for service providers. If they decided to continue policing content and exercising prior restraint on “inappropriate” or possibly illegal information which their users posted, they made themselves vulnerable to a potential defamation lawsuit. Since millions of users contributed to their network on a daily basis, it seemed more likely that fear of prosecution would inspire Prodigy and other ISPs like it to adopt a more hands-off approach which precluded them from moderating even the most objectionable or unlawful content. The legal fees and possible settlements that their current approach threatened was surely the more expensive route to maintain.

¹⁵ 23 Media L. Rep. 1794, 10 (N.Y.S. 1995).

¹⁶ 23 Media L. Rep. 1794, 11 (N.Y.S. 1995).

The Cyberporn Panic of 1995

Congress, it seems, was also worried about Internet service providers (ISPs) abrogating responsibility for fear of becoming a publisher like Prodigy. At the time that Prodigy's motion was being denied, a piece of legislature known as the Telecommunications Act of 1996 was being debated in Congress. During this debate, a provision known as the Communications Decency Act was offered as a solution to the growing concerns regarding the prevalence and easy access to indecent and pornographic material in cyberspace. Their efforts were particularly targeted towards protecting minors, who they feared could be accidentally exposed to "indecent" material while browsing the Internet.¹⁷ This increased effort is thoroughly illustrated in a *Time Magazine* story published in the July 3, 1995, issue.¹⁸ The cover, a picture of a shocked child at a computer with the word "CYBERPORN" bold and centered, caught the attention of readers. The story's content was based largely on a study conducted by an electrical engineering student from Carnegie-Mellon University named Martin Rimm. What became known as "The Rimm Study" or "Rimm Report" explained just how bad the cyberporn problem had supposedly become, citing that over eighty percent of the photos on the Internet were pornographic in nature.¹⁹ While the study did have several

¹⁷ 47 U.S. C. A. §223(a) (Supp. 1997).

¹⁸ Philip Elmer- Dewitt, "On A Screen Near You: Cyberporn," *Time Magazine*, July 3, 1995.

¹⁹ Marty Rimm, "Marketing Pornography on the Information Superhighway: A Survey of 917,410 Images, Descriptions, Short Stories, and Animations Downloaded 8.5 Million

methodological issues and biases (it was never submitted for peer review and Rimm only searched for photos on adult bulletin boards), a spark had still been ignited in Congress.

It is important to note that the Cyberporn Panic created an interest in regulating Internet pornography and not obscenity. There was no need to adopt new laws against cyber obscenity because such speech is already illegal. In the Supreme Court decision of *Roth v. United States* (1957), Justice William Brennan wrote that the Court had “always assumed that obscenity is not protected by the freedoms of speech and press.”²⁰

Congress wanted to target non-obscene speech that was indecent, pornographic, or harmful to minors. Pornography was legal in the physical world, but the Internet truly allowed it to flourish as an industry and grow as the Internet itself grew. Whereas in the real world laws that prevented minors from accessing this type of material kept the issue under control, the Internet provided children with easy access to a seemingly unlimited and continuously expanding porn industry. It is because of this distinction that Congress found it necessary to create special legislation to combat the issue of pornography in this relatively new medium.

The CDA sought to prohibit any “communication which is obscene or indecent” when the recipient of such information is “under 18 years of age” even if said recipient “initiated the communication.”²¹ The CDA went on to explain that any “communication that, in context, depicts or describes, in terms patently offensive as measured by

Times by Consumers in Over 2000 Cities in Forty Countries, Provinces, and Territories,” *Georgetown Law Journal* 83 (June 1995), 1849.

²⁰ *Roth v. United States*, 354 U.S. 476 (1957).

²¹ 47 U.S. C. A. §223(a) (Supp. 1997).

contemporary community standards, sexual or excretory activities or organs” was also prohibited.²² If a website took “good faith” actions to restrict access to minors or require some sort of proof of age such as a credit card number, under the CDA they would be able to form an affirmative defense against judicial action.²³

After the *Stratton Oakmont* decision, Congress feared that ISPs would be encouraged to allow the very content they were trying to eliminate to exist on their servers so that they could avoid being considered a publisher unworthy of certain legal protections. Ideally, Congress wanted ISPs to vigilantly police this type of expression and cooperate with the effort to clean up cyberspace. *Stratton Oakmont*, however, held out the possibility that regulating content would qualify an ISP for publisher status. In response to this issue, Congress added Section 230 to the CDA which granted ISPs immunity from liability. While the Act began “with the Congressional findings and a statement of policy behind the Act,” the third section became the “focal point” as it discussed this immunity in detail.²⁴ Section 230 of the CDA reads:

(c) Protection for “good samaritan” blocking and screening of offensive material

(1) Treatment of publisher or speaker

²² 47 U.S. C. A. §223(a) (Supp. 1997).

²³ 47 U.S. C. A. §223(a) (Supp. 1997).

²⁴ Cyrus Sarosh Jan Manekshaw, “Liability of ISPs: Immunity from Liability under the Digital Millennium Copyright Act and the Communications Decency Act,” *Computer Law Review & Technology Journal* 10 (Fall 2005), 106.

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.

(2) Civil liability

No provider or user of an interactive computer service shall be held liable on account of—

(A) any action voluntarily taken in good faith to restrict access to or availability of material that the provider or user considers to be obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable, whether or not such material is constitutionally protected; or

(B) any action taken to enable or make available to information content providers or others the technical means to restrict access to material described in paragraph (1).²⁵

Before the law could be enforced, the American Civil Liberties Union and other organizations challenged the provisions of the CDA directed toward indecent speech and speech that is harmful to minors. While the ACLU and its fellow plaintiffs found no issue with outlawing “obscene” material from the Internet, they felt that the terms “indecent” and “patently offensive” were vague and overbroad. As such, the mandates of the CDA might reach discussions about rape, sexual health, gay and lesbian issues, and the AIDS virus. The American Library Association (ALA) joined the ALCU as a plaintiff because they felt that many great works of literature which contained

²⁵ 47 U.S.C. §230(c).

controversial or adult themes would be censored, as well. Furthermore, since indecent speech received constitutional protection in the real world, the ACLU felt that the same rules should apply in the cyber world.

The Supreme Court voted 7-2 in favor of the ACLU and its fellow plaintiffs in *Reno v. ACLU*, citing the CDA's vagueness and overbreadth as arguments for its unconstitutionality.²⁶ Specifically, the Supreme Court cited the lack of a definition for the terms "indecent" and "patently offensive" as problematic. As Justice John Paul Stevens explains in the *Reno* decision, "The severity of criminal sanctions may well cause speakers to remain silent rather than communicate even arguably unlawful words, ideas, and images."²⁷ The content of the CDA put speech about AIDS, rape, homosexuality, sexual health, and other controversial issues at great risk, and furthermore, the Court believed that its overbroad language suppressed speech that, although harmful to minors, was still legally acceptable for adults.²⁸ This decision is particularly noteworthy because the Court recognized clearly that the Internet should receive a full measure of First Amendment protection. Their decision, however, only invalidated the parts of the CDA dealing with "indecent" content, and the Court's ruling did not affect the rest of the Telecommunications Act, including Section 230. From then on, ISPs could no longer be considered publishers and were free to pursue efforts to police and maintain their content.

²⁶ *Reno v. American Civil Liberties Union*, 521 U.S. 844, 870 (1997).

²⁷ 521 U.S. 844, 871 (1997).

²⁸ 521 U.S. 844, 879-880 (1997).

The *Reno* decision also created an interesting paradox, though. At its inception, the CDA was an amendment to the Telecommunications Act of 1996 that was supposed to regulate more speech. Responding to the cyberporn panic, Congress intended to eliminate content that was producing unwanted results. Section 230 itself was created to encourage ISPs to police their content and exercise editorial control when that content became inappropriate or unsavory without being considered a publisher liable for damages. After the Supreme Court's ruling, though, the opposite resulted. With the provisions barring "indecent" and "patently offensive" material struck down, the CDA became a law which actually protected speech. Since Section 230 remained intact after the *Reno* decision, ISPs were still immune even if they chose not to exercise their right to censor or police third-party content. As it began to be applied in court rooms across the nation, Section 230 inevitably produced some interesting results.²⁹

Zeran v. AOL

The first case which would test the strength of Section 230 came swiftly. On April 19, 1995, the Alfred P. Murrah Federal Building was bombed, taking 168 lives and injuring more than 800 individuals in the building. This event became known as the Oklahoma City bombing, at that point in history the worst act of terrorism on United States soil. Since the building was home to the America's Kids Day Care Center,

²⁹ See, for example, Suman Mirmira, "V. Business Law: 1. Electronic Commerce: a) Internet Service Provider Liability: *Lunney v. Prodigy Services Co.*," *Berkeley Technology Journal* 15 (2000), 437-438.

nineteen children were killed as a result of this tragedy. The incident made national headlines and received round the clock coverage for several days in various news markets. Six days later, a message was posted on an America Online (AOL) message board advertising Oklahoma City bombing t-shirts for sale. Interested buyers were instructed to contact the user “Ken ZZ03,” and a phone number and email address were included in the post.

Not surprisingly, these t-shirts were in extremely poor taste. The advertised slogans poked fun at what had just occurred and alluded to the children that had been victims in the attack. By the end of this message board incident, five different slogans were published ranging from “Visit Oklahoma—it’s a blast” to “Finally a day care center that keeps the kids quiet...Oklahoma 1995.” A radio DJ from the station KXRO in Oklahoma City named Mark Shannon found out about this message board advertisement, and, completely outraged, he encouraged listeners to contact “Ken” and harass him for making light of such a terrible tragedy. The problem was, Ken Zeran, who was now receiving threatening and admonishing emails and phone calls, allegedly had nothing to do with the creation or publication of this ad. After complaining for four days to AOL, the message was eventually removed. A second message was almost immediately posted with new slogans and the same contact information, but AOL ultimately deleted this post, as well.³⁰

Zeran sued AOL, alleging that they had failed to remove the initial post in a timely manner and appeared negligent when a second post with almost identical content made its way back on to the message board. His suit also seemed practical considering

³⁰ Summary derived from *Zeran v. America Online*, 129 F.3d 327 (4th Cir. 1997).

the identity of his defamer was still unknown and a suit against a large company like AOL could possibly encourage the ISP to divulge this information or investigate the whereabouts of the user in question. When this case reached the Fourth Circuit Court of Appeals, it seemed as if no legal argument could be made that would allow Zeran to win a suit brought against AOL, an Internet service provider. After all, Section 230 clearly stated that AOL was immune from liability even when it exercised editorial control or regulated its content. The Fourth Circuit thoroughly outlined this point in the first section of their decision.

Congress enacted Section 230 to remove the disincentives to self-regulation created by the *Stratton Oakmont* decision. Under that court's holding, computer service providers who regulated the dissemination of offensive material on their services risked subjecting themselves to liability, because such regulation cast the service provider in the role of publisher. Fearing that the specter of liability would therefore deter service providers from blocking and screening offensive material, Congress enacted Section 230's broad immunity "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." In line with this purpose, Section 230 forbids the imposition of publisher liability on a service provider for the exercise of its editorial and self-regulatory functions.³¹

Anticipating this line of argument, Zeran tried to circumvent Section 230 by arguing that distributors could be held liable if they had notice that they were distributing

³¹ 129 F.3d 327, 331 (4th Cir. 1997).

defamatory content. While *Cubby v. CompuServe* seemed to imply that distributors could not be held liable either as previously discussed, Zeran alleged that this was true “unless it is proven at a minimum that [ISPs] have actual knowledge of the defamatory statements upon which liability is predicated.”³² Since he had “provided AOL with sufficient notice of the defamatory statements appearing on the company’s bulletin board,” Zeran claimed that AOL had stepped out of the realm of Section 230 and that distributor liability should apply in this situation.³³ The Fourth Circuit Court of Appeals was not impressed with Zeran’s argument, however, and expressed that he had missed the point of Section 230 and what it sought to achieve. The opinion of the court revealed where he had gone wrong.

Zeran fails, however, to understand the practical implications of notice liability in the interactive computer service context. Liability upon notice would defeat the dual purposes advanced by Section 230 of the CDA. Like the strict liability imposed by the Stratton Oakmont court, liability upon notice reinforces service providers’ incentives to restrict speech and abstain from self-regulation.³⁴

The Fourth Circuit felt that this sort of distributor liability defeated the intended purpose of Section 230 in the first place. Section 230 was created to encourage ISPs to regulate their content and prevent an unnecessary restriction on free expression. If ISPs felt that they could be legally liable for any of the millions of actions that take place on their networks, they could implement strict guidelines which could chill non-

³² 129 F.3d 327, 331 (4th Cir. 1997).

³³ 129 F.3d 327, 331 (4th Cir. 1997).

³⁴ 129 F.3d 327, 333 (4th Cir. 1997).

objectionable material or they could let users run wild and post anything while turning a blind eye. The concept of becoming legally liable once an affected party notifies the company of something they feel is objectionable seemed similarly unreasonable to the Fourth Circuit. If all a user had to do was complain to have something removed, speech which is not defamatory or illegal could be chilled if the ISP wishes to be safe rather than liable. A large company like AOL could potentially receive thousands of complaints a day from all of its users, imposing an unnecessary burden which could encourage it to shut down parts of its services. The *Zeran* decision seemed to affirm that Section 230 was good law with plenty of staying power.

Yet AOL was what could commonly be considered an Internet service provider. Their business model revolved around granting their customers access to the Internet and its various features through their computer software program and subscription fees. The courts would not stop at this simple interpretation of the definition of a service provider, though, and Section 230's reach would only continue to expand well beyond this traditional realm. Soon the idea of an Internet service provider would translate in a very literal sense to locations which actually physically granted users access to the Internet. As these definitions and the court's perception of the Internet's role in society began to grow, so did the breadth of Section 230 immunity.

In 2001, a district court broke the mold when it confirmed that Kinko's, commonly considered to be just in the copy and printing business, was an Internet service provider. Michael Neustel invented a software program called PatentWizard, which marketed itself as an easy way for fellow inventors to patent their inventions and complete the paperwork the federal government considered necessary to do so. Neustel

hosted an Internet chat room in 2000 to discuss the newest version of PatentWizard with current and prospective customers. During the chat session, a user identified as “Jimmy” began to aggressively criticize the PatentWizard software. Since “Jimmy” made his comments from a computer he purchased time on at Kinko’s, Neustel asked that they divulge the true identity of the user. Kinko’s, however, did not keep records of individuals who used their network to access the Internet and had no resources which would allow them to assist in the identification of “Jimmy.” As a result, Neustel sued Kinko’s for negligent behavior, failure to maintain records, and “aiding and abetting” defamation which damaged his product’s and own personal reputation.³⁵

District Judge Lawrence Piersol dismissed the case on the grounds that Kinko’s was immune under Section 230. “Information originating with a third-party user,” he clarified, is not the responsibility of Kinko’s.³⁶ Kinko’s may have indirectly disseminated “Jimmy’s” message by providing him with the means to do so, but this was at the very core of what Section 230 was created to protect. Federal immunity prevented “any cause of action” from legally sticking against this Internet service provider.³⁷ Judge Piersol did briefly mention a small dilemma that Section 230 created, though. While he acknowledged that any person’s ability to remain anonymous on the Internet (which had obviously taken place in the PatentWizard incident) did promote the “robust communication” which could be “the Internet’s most important contribution to society,” he also realized that the ability to “link an individual’s online identity to his or her

³⁵ Summary derived from *PatentWizard v. Kinko’s*, 162 F. Supp. 2d 1069 (D. S.D. 2001).

³⁶ 162 F. Supp. 2d 1069, 1071 (D. S.D. 2001).

³⁷ 162 F. Supp. 2d 1069, 1071 (D. S.D. 2001).

physical self” would be paramount in preventing this kind of expression from “causing harm in the real world.”³⁸ Rather than discussing this issue further, though, Judge Piersol simply states that when this conflict is properly resolved it will “shape the content of communication over the Internet.”³⁹ He resigns his thoughts by saying that for now, he will defer to the side of “robust communication” and leave that issue for another court to consider.⁴⁰

While the *Zeran* case produced some tough results for Zeran himself, it was not surprising when the courts interpreted the language of Section 230 to grant America Online immunity from a defamation lawsuit. As an Internet service provider with a great deal of customers, it is unreasonable to expect the company to monitor the constant activity of all of its users no matter how egregious their behavior may be. The *PatentWizard* case stretched the power of Section 230 even further when Kinko’s was given the Internet service provider distinction because it provided its customers with access to computers that were connected to the Internet. Although this was the first time that a company without a primary stake in Internet activity was given this distinction, it falls in line with the idea that such providers should not be held responsible for the words and actions of third-party users who happen to use their networks. *PatentWizard* pushed the boundaries of Section 230 beyond the groundwork *Zeran*, but this would not be the last time that the law’s scope would be expanded into previously uncharted areas of the web.

³⁸ 162 F. Supp. 2d 1069, 1071 (D. S.D. 2001).

³⁹ 162 F. Supp. 2d 1069, 1072 (D. S.D. 2001).

⁴⁰ 162 F. Supp. 2d 1069, 1072 (D. S.D. 2001).

The *Zeran* Line

So far the types of cases that have been discussed deal with companies known as Internet service providers (ISPs). CompuServe, Prodigy, AOL, and Kinko's literally provide Internet service to their customers. As Section 230 gained momentum, though, the question became whether or not it would extend beyond these traditional ISPs to Internet content providers. For example, today there are companies and websites (like Amazon.com) that provide both service and their own original content. There are also websites which facilitate the content their users provide and encourage them to provide more of it. As these raise separate concerns, each will be considered in the paragraphs that follow.

Internet Content Providers

Internet service providers were certainly protected from liability—*Cubby* and *Zeran* had proved that—but as the online world continued to develop and increase in popularity, the courts seemed to shift their attention to Internet content providers (ICPs). In the *Zeran* case, AOL was sued for content which was posted anonymously by one of the users on its networks. In the case of content providers, however, various service providers and websites began supplying content that they produced themselves which could arguably qualify them as publishers. Whether or not ICPs would be held responsible for posting this content became the next question for the courts to tackle. The

case *Blumenthal v. Drudge* (D.D.C. 1998) signaled this change. Since the need for companies like CompuServe, Prodigy, and even AOL to provide individual networks and service seemed to be fading, the industry shifted its attention to providing interactive content for Internet users to access and often times contribute to. Needing to stay relevant in such a rapidly developing market, AOL began to engage in this practice.

Matt Drudge was an Internet journalist famous for what became known as the *Drudge Report*. It began in 1994 as a weekly subscriber-based publication sent by e-mail which contained news stories, gossip, and columns written by Drudge himself which focused on Hollywood and Washington, D.C. Drudge is perhaps most famous for being the first to break the news of the affair between President Bill Clinton and Monica Lewinsky, after *Newsweek* refused to publish the information. Even before the Clinton-Lewinsky story, though, Drudge and America Online entered into a contractual agreement which allowed AOL users to view the *Drudge Report* every week. On August 10, 1997, Drudge submitted that week's issue of the *Drudge Report*, the main topic being Sidney Blumenthal, an assistant and senior adviser to President Clinton. Among the comments and allegations made about Blumenthal by Drudge was a claim that court records showing Blumenthal's violence against his wife could exist. The exact text of this issue of the *Drudge Report* is as follows:

There are court records of Blumenthal's violence against his wife, one influential republican, who demanded anonymity, tells the DRUDGE REPORT.

If they begin to use [Don] Sipple and his problems against us, against the Republican Party ... to show hypocrisy, Blumenthal would become fair game.

Wasn't it Clinton who signed the Violence Against Women Act?

[There goes the budget deal honeymoon.]

One White House source, also requesting anonymity, says the Blumenthal wife-beating allegation is a pure fiction that has been created by Clinton enemies. [The First Lady] would not have brought him in if he had this in his background, assures the well-placed staffer. This story about Blumenthal has been in circulation for years.

Last month President Clinton named Sidney Blumenthal an Assistant to the President as part of the Communications Team. He's brought in to work on communications strategy, special projects themeing -- a newly created position. Every attempt to reach Blumenthal proved unsuccessful.⁴¹

Drudge quickly retracted the story since there was little evidence that this spousal abuse had actually occurred and few sources could be confirmed. Unmoved by Drudge's retraction of the story, Blumenthal sued Drudge and AOL for \$30 million.⁴²

The case against AOL was immediately dismissed by the district court. While the court acknowledged that "if it were writing on a clean slate" it would agree with Blumenthal since "it would seem only fair to hold AOL to the liability standards applied to a publisher or, at least, . . . to a distributor," Judge Paul Friedman acknowledged that the law made by Congress—namely, Section 230—still provided immunity.⁴³ It provided immunity, the court specified, "even where the interactive service provider has an active,

⁴¹ *Blumenthal v. Drudge*, 992 F. Supp. 44 (D.D.C. 1998).

⁴² Summary derived from 992 F. Supp. 44 (D.D.C. 1998).

⁴³ 992 F. Supp. 44, 54 (D.D.C. 1998).

even aggressive role in making available content prepared by others.”⁴⁴ ISPs would continue to enjoy immunity as an incentive to regulate their content and police objectionable material “even where the self-policing is unsuccessful or not even attempted.”⁴⁵ This would also continue, this case seemed to imply, when ISPs transformed into ICPs.

Since Section 230 only provided immunity for AOL, Blumenthal continued to pursue his suit against Drudge. After five years of litigation, Blumenthal dropped the suit and actually ended up having to pay Drudge \$2,500 for missing a deposition. Had he continued, it is possible that a court could have found Drudge guilty of defamation, a fact which only further illuminates the extraordinary protection that Section 230 provides AOL and other companies like it. A company like AOL will always leave such a situation free from any sort of responsibility, but people like Matt Drudge, even if they are employees of the a company like AOL and their content is directly published and endorsed by that company, receive no such remedy or shield.

AOL became the subject of yet another Section 230 case in *Ben Ezra, Weinstein, and Company v. America Online* (10th Cir. 2001) when the “Quotes and Portfolios” section of their area devoted to finance and investments was found to contain false information. The stock information provided on this page was compiled by a third party, and AOL exercised no editorial control prior to posting. For whatever reason, the “Quotes and Portfolios” service that AOL made available to its subscribers listed incorrect quotes regarding the price and value of a company known as Ben Ezra,

⁴⁴ 992 F. Supp. 44, 54-55 (D.D.C. 1998).

⁴⁵ 992 F. Supp. 44, 55 (D.D.C. 1998).

Weinstein's stock. Believing that this had led investors to lose faith or even overlook their company's potential, Ben Ezra, Weinstein sued AOL for defamation.⁴⁶

AOL filed for summary judgment in a district court, and the motion was immediately granted citing Section 230 as the main argument. Ben Ezra, Weinstein appealed all the way to the Tenth Circuit, but the judges agreed with the district court. "Congress clearly enacted Section 230 to forbid the imposition of publisher liability on a service provider for the exercise of its editorial and self-regulatory functions," the Tenth Circuit asserted.⁴⁷ "By deleting the allegedly inaccurate stock quotation information, Defendant was simply engaging in the editorial functions Congress sought to protect."⁴⁸ Even if AOL published inaccurate content on their server, the court clarified, Section 230 precluded them from any sort of liability.⁴⁹

What separates this case from *Blumenthal* and illustrates just how quickly Section 230 immunity was expanding, however, is the nature of the information in question. In the *Blumenthal* case, Matt Drudge published information which was faulty and may have stemmed from unreliable sources, but it could be argued that the story could have been true or at the very least Drudge believed it to be true when he initially published it. Some of the content of his posting could also be read as the author's opinion rather than actual statements of fact. In the *Ben Ezra* case, though, AOL published information that was

⁴⁶ Summary derived from *Ben Ezra, Weinstein and Company v. America Online*, 206 F.3d 980 (10th Cir. 2001).

⁴⁷ 206 F.3d 980, 986 (10th Cir. 2001).

⁴⁸ 206 F.3d 980, 986 (10th Cir. 2001).

⁴⁹ 206 F.3d 980, 986 (10th Cir. 2001).

flat out false. The stock figures were completely inaccurate and the numbers they provided were an inaccurate reflection of the company's performance. The fact that AOL still received full immunity demonstrated the growing reach of Section 230. Even if an Internet content provider printed false information, they could not be held responsible for the harm it potentially posed to an outside party. As the next set of websites will demonstrate, those responsible for maintaining the Internet would be able to continue to expand their control beyond providing their own content and still enjoy the same protection.

Internet Content Facilitators

In addition to extending Section 230 immunity to Internet content providers, the courts also began to expand the definition of what could be considered an ISP or ICP. The major cases up to this point involved companies like AOL and CompuServe which fit the traditional realm of ISP immunity despite the fact that some companies were beginning to become more proactive in their content creation. A new brand of websites, best reflected in the term "Internet content facilitators" (ICFs), were not only publishing content created by their users or hired outside parties, they were creating the structured mechanisms by which this content was submitted and facilitating its outcome or final form. Whether in the structure of an online forum, dating service, or rating system, these websites encourage users to interact with their site and rely on their visitors to provide a crucial component of the site's content.

The courts signaled this continued expansion of Section 230 when a man named Jerome Schneider brought a suit against the online shopping site Amazon.com. Schneider was the author of several books on taxation and asset protection which were sold on the Amazon site. As a service to its users, Amazon.com allows customers to post reviews on all of its products, including its book selection. Near the bottom of every book's individual web page, Amazon encouraged users and provided a form that allowed them to state their opinions or experiences (positive or negative) regarding the product. When Amazon users began to post negative reviews in reference to Schneider's books, he petitioned the site to take the reviews down. They did not, and consequently Schneider sued them for defamation. In his suit he did not fault Amazon.com for initially posting the negative reviews, but for failing to remove these posts after "promising" to do so and actually reposting them rather than deleting them.⁵⁰

In *Schneider v. Amazon.com* (Ct. of Appeals, Wash., 2001), the Washington State Court of Appeals dismissed Schneider's case on Section 230 grounds. In their decision, the court reminded readers that Section 230 was a "Good Samaritan" law which allowed an interactive computer service to do as they pleased with their content.⁵¹ Amazon.com did have certain rules and guidelines for posting reviews on their site, and they also made it clear that certain posts would be removed if they violated such terms and conditions that are agreed upon when an individual signs up to use the service. When and how they decided to follow through with these policies, though, the court felt was entirely up to

⁵⁰ Summary derived from *Schneider v. Amazon.com*, 31 P. 3d 37 (Ct. of Appeals, Wash., 2001).

⁵¹ 31 P. 3d 37, 41 (Ct. of Appeals, Wash., 2001).

Amazon.com. “Assuming Schneider could prove existence of an enforceable promise to remove the comments, Schneider’s claim is based entirely on the purported breach—failure to remove the posting—which is an exercise of editorial discretion,” the court explained.⁵² “This is the activity” that Section 230 “seeks to protect.”⁵³

While *Schneider* expanded the scope of Section 230 protection by allowing website owners to create the actual form for users to submit their content, this notion would be pushed even further when a website known as Matchmaker.com was brought before the courts. While Matchmaker also provided a form for users to submit their content, theirs was much more organized and structured and offered specific spaces and questions for users to fill in targeted information about themselves. The website allowed users trial periods, where they could create a profile and explore the site’s services before committing to any sort of program or payment plan. When an individual wanted to create a profile, Matchmaker provided an online form for them to fill out which included spaces for new members to list their contact information, hobbies, sexual interests, and other personal facts. Matchmaker would then publish the individual’s responses as a profile on their site, and other members could view the material and contact the person if they were romantically interested. Without new users to participate in Matchmaker’s free trial and create new profiles, the dating website would cease to function properly. An anonymous user in Berlin accepted one of these trials, but created a personal profile for Christine Carafano, an actress more commonly known by the stage name Chase Masterson. Carafano’s character Leeta on “Star Trek: Deep Space Nine” was very popular with

⁵² 31 P. 3d 37, 40 (Ct. of Appeals, Wash., 2001).

⁵³ 31 P. 3d 37, 41 (Ct. of Appeals, Wash., 2001).

viewers, and so the user created a profile complete with two pictures, a brief filmography, and her actual home address and up to date contact information. The user profile (named “Chase 529”) also listed several interests with obvious sexual implications and claimed that Carafano wished to be sexually dominated by her partner. Almost immediately, Carafano began receiving threatening and sexually violent messages on her voice mail. Her publicist learned of the Matchmaker profile, reported its illegitimacy and the resulting harassment to the site manager, and the profile was eventually blocked and then deleted altogether.⁵⁴

It seems that the identity of the German poster could have been ultimately obtained by Carafano, but the thought and overall process of pursuing a suit in German court with possible international proceedings and varying laws seemed incredibly daunting and costly. Due to the fact that Matchmaker.com had failed to properly screen the profile before publishing its contents and accepting a new user and because they had been slow to remove the “Chase 529” profile even after the resulting harassment, Carafano sued Metrospash, the owners of the Matchmaker site. As a result of Section 230, Carafano quickly lost in federal court. She did appeal to the Ninth Circuit, but in *Carafano v. Metrospash.com*, the results were much of the same. Section 230, the court wrote, granted full immunity under the law “so long as a third party willingly provides the essential published content.”⁵⁵ Matchmaker, they claimed, could not even be

⁵⁴ Summary derived from *Carafano v. Metrospash.com*, 339 F.3d 1119 (9th Cir. 2003).

⁵⁵ 339 F.3d 1119, 1124 (9th Cir. 2003).

considered an ICP (the younger sibling of the ISP) since a profile on their site could not possibly exist unless a third party provided the information essential to its creation.⁵⁶

Section 230 has been expanded to include non-traditional Internet service providers like Kinko's, service providers that began producing their own content whether it was true or not, and now websites that facilitated the creation of questionable material by creating sometimes extensively designed forums. These forums could take the form of a simple blank space for visitors to express themselves however they deemed appropriate like the Amazon reviews or, in the case of Matchmaker, the forums could be more of a structured form with specific spaces for things like hobbies, interests, or work information. As the next case will exemplify, however, the role that website owners and creators play in structuring these forums does have its limits. While Section 230 immunity had become quite powerful by this point, one website would discover that it was not absolute.

The Roommates Exception

Such a broadening definition of immunity had produced some difficult results in the past and made it increasingly difficult for individuals to circumvent the strength of a Section 230 argument. To date, there is only one known instance where a Section 230 defense was rejected by the courts. Roommates.com is a website that provides an online roommate matching and searching service for individuals across the country. Membership is absolutely free, but in order to use the site's services, interested users are

⁵⁶ 339 F.3d 1119, 1124 (9th Cir. 2003).

required to create a profile and answer a series of questions. Those questions required the user to identify his or her sex, sexual orientation, and whether or not he or she would be bringing children to the household. There was also a space available for “additional comments” which the site member could fill with other useful information regarding their roommate preferences. While filling in any additional information was not a membership condition, answering the first three questions by means of a drop-down menu was. As of 2008, Rommates.com had over 150,000 active listings on its website and received over one million “hits” or site visits a day from individuals searching for roommates or posting housing opportunities. The Fair Housing Councils of the San Fernando Valley and San Diego sued Roommates.com in federal court on the grounds that Roommates had violated the Fair Housing Act (FHA) and other California housing discrimination laws by forcing its members to answer identifying questions about themselves that would aid others in discriminating against them. The district court held that Roommates.com was immune under Section 230, but, for the first time ever, the Ninth Circuit Court of Appeals did not entirely agree.⁵⁷

Referencing the three questions and the drop-down menu format, Chief Judge Alex Kozinski wrote, “By requiring subscribers to provide the information as a condition of accessing its service, and by providing a limited set of pre-populated answers, Roommates becomes much more than a passive transmitter of information provided by others; it becomes the developer, at least in part, of that information.”⁵⁸ Since Section

⁵⁷ Summary derived from *Fair Housing Council of San Fernando Valley v.*

Roommates.com, LLC, 521 F.3d 1157 (9th Cir. 2008).

⁵⁸ 521 F.3d 1157, 1166 (9th Cir. 2008).

230 provides immunity only if the service provider does not “create or develop” the content in question “in whole or in part,” the court reasoned that immunity did not apply in this situation.⁵⁹ Although the information was being provided by the website’s members, Judge Kozinski explained that the offending content was still a collaborative effort involving Roommates.com. “The projectionist in the theater may push the last button before a film is displayed on the screen,” he clarified, “but surely this doesn’t make him the sole producer of the movie.”⁶⁰

In reference to the “additional comments” section, however, the court felt that since “Roommates publishes these comments as written” and only provides a blank space for users to fill with no additional instruction, Section 230 would protect Roommates.com from liability if any discriminatory postings were made using this particular mechanism.⁶¹ This section of the website, Judge Kozinski elaborated, was “precisely the kind of situation for which Section 230 was designed to provide immunity” and similar to the situation presented in the *Carafano* case.⁶² The Ninth Circuit sent the case back to the lower courts to determine whether the FHA and other California housing laws had been violated, with the note that if the court found the questionnaire portion of the site to be discriminatory and in violation of these laws, no Section 230 immunity should be granted to Roommates.

⁵⁹ 47 U.S.C. §230(f)(3).

⁶⁰ 521 F.3d 1157, 1167 (9th Cir. 2008).

⁶¹ 521 F.3d 1157, 1173 (9th Cir. 2008).

⁶² 521 F.3d 1157, 1174 (9th Cir. 2008).

While this case seems to shake up the *Zeran* line, in reality it does not depart from the previous group of cases. Roommates.com was simply held responsible for perhaps over-extending its involvement in its site's content, and had the website simply left some of its questions or profile sections more open-ended, it almost certainly would have received the same sweeping immunity as its predecessors. Two other cases, *Batzel v. Smith* and *Barrett v. Rosenthal*, came very close to making more significant dents in Section 230's seemingly impenetrable immunity. *Batzel* involved resending defamatory content over an online network using an email listserv, and the *Barrett* case entailed a woman who reposted a defamatory statement on an online message board.⁶³ While the lower courts found both individuals guilty and unprotected by Section 230, on appeal both decisions were reversed. *Roommates.com* stands as the sole case where Section 230 immunity was rejected, yet its decision does not affect the outcome of any past cases and will have very little affect on Section 230 case law as a whole. Section 230 immunity is very narrowly denied in this situation and only one aspect of the website's forum was deemed vulnerable. The principles set forth in *Schneider* and *Carafano* still apply in this situation and remain good law, and the fact that the site's "additional comments" section was not deemed actionable and did receive immunity is consistent with these previous decisions and the Section 230 casework as a whole.

⁶³ See *Batzel v. Smith*, 2001 U.S. Dist. LEXIS 11921 (C.D. Cal., July 25, 2001), affirmed in part and vacated in part, 333 F.3d 1018 (9th Cir. 2003) and *Barrett v. Rosenthal*, 112 Cal. App. 4th 749, 763 (1st Dist., Div. 2, 2003), superceded by 9 Cal. Rptr. 3d 142 (Cal. App. 2004).

Extending beyond Defamation

Defamation is not the only area of law which has found refuge under the umbrella of Section 230 immunity. In fact, the wide variety of speech that has found protection under Section 230 is a testament to how liberally the courts have applied it since Congress created it over a decade ago. Section 230 has been interpreted so broadly that it has even protected some of the kinds of speech which it was originally intended to regulate and prevent.

In 1998, a case dealing with online child pornography—precisely the type of material Section 230 was originally created to combat—was brought before a Florida court. A man by the name of Richard Russell lured an 11-year-old boy and two other minors to a location where he videotaped and photographed them engaging in sexual activities with each other. Russell then attempted to market and sell this material in AOL chat rooms. He was eventually arrested and pled guilty to federal criminal charges based on these actions, but Jane Doe, the mother of the 11-year-old boy, filed an \$8 million lawsuit against AOL. She felt that they had behaved negligently and should be held responsible in some way for providing a service which allowed pedophiles to lure young children and exploit them. Doe argued that several users had complained about Russell's behavior and violation of AOL's terms of service and user agreements, but nonetheless his service was never suspended nor was he warned that his behavior was inappropriate.⁶⁴

In *Jane Doe v. America Online*, the court decided that Russell's postings and behavior on the AOL network were “analogous to the defamatory publication at issue in

⁶⁴ Summary derived from *Jane Doe v. America Online*, 783 So. 2d 1010 (Fla. 2001).

the *Zeran* decisions.”⁶⁵ Although Florida has “criminal statutes prohibiting the distribution of obscene literature and computer pornography,” the court responded that “Section 230 preempts Florida law as to causes of action based in negligence against an Internet Service Provider.”⁶⁶ Although the material published on AOL by Russell was undoubtedly illegal, Section 230 prevented AOL from any liability. What was once a provision of an anti-pornography and indecency campaign was now the very “shield” that ISPs were using to escape any responsibility or duty to police their content.⁶⁷

In a similar case known as *Julie Doe v. Myspace.com*, a 13-year-old girl created an account on the Myspace network by claiming she was 18 during the registration process. She began contacting a 19-year-old male who agreed to meet her, and during their meeting he allegedly sexually assaulted her. The man was arrested and charged with sexual assault, but the girl’s family decided to sue Myspace for making it so easy for minors to create profiles on their site and become vulnerable to online predators. Understanding the limitations that Section 230 presented, the family made it clear in their suit that they did not wish to punish any content available on the Myspace website. Rather, they wanted to hold Myspace responsible for not having safety measures in place to protect minors. It was their hope that the court would limit Section 230 protection to

⁶⁵ 783 So. 2d 1010, 1017 (Fla. 2001).

⁶⁶ 783 So. 2d 1010, 1013 (Fla. 2001).

⁶⁷ 783 So. 2d 1010, 1019 (Fla. 2001).

areas related to defamation and not their own situation which involved no third-party content.⁶⁸

Unfortunately for the Doe family, the case was dismissed. “Despite Plaintiffs’ arguments to the contrary,” Judge Sam Sparks wrote, “the court finds *Zeran* and its rationale to be applicable to the case at hand.”⁶⁹ The court felt that it was unreasonable for Myspace to know that sexual predators existed on their network and they did not feel it was Myspace’s responsibility to uncover this information. Section 230 had once again prevented a website from being penalized even when it seemed that a child’s life had been harmed.

Although both of these cases have outcomes that are difficult and uncomfortable at best, different results would create another set of problems. While it is undesirable that minors should fall victim to online predators, Congress itself sought to protect minors when it enacted the CDA over a decade ago, holding America Online or Myspace responsible may not be the solution either. What lies at the heart of this conundrum is a public policy issue which pits freedom of speech against the right to privacy and protection from these types of predators on the Internet. These cases seem to imply that free expression is valued more in this country and in its system of government than the latter, but the strict application of Section 230 in these cases is not without its reasons. Had Jane and Julie Doe prevailed in their lawsuits against AOL and Myspace, a dangerous precedent would have been set. If AOL and Myspace knew that they could be

⁶⁸ Summary derived from *Julie Doe v. Myspace.com*, 474 F. Supp. 2d 843 (W.D. Tex. 2007).

⁶⁹ 474 F. Supp. 2d 843, 848 (W.D. Tex. 2007).

held liable for sexual predators committing crimes on their servers, the thought of having to deal with a wave of lawsuits resulting from the various activities of its users could prove so daunting that they would either have to shut down or severely curtail their services. Having to monitor everything and everyone is not a profitable or manageable business scheme, and soon a few offenders could eliminate the opportunity for everyone to express themselves.

Beyond defamation and situations related to the safety of minors, Section 230 has also been used by the courts in cases related to the use of Internet filters. *Kathleen R. v. City of Livermore* is a case which illustrates this distinctive approach to the law. As is common in various libraries throughout the country, the Livermore Public Library provides free Internet access to its members. A 12-year-old boy used this service to download sexually explicit photos on to a floppy disk which he would later print out at an unsuspecting family member's residence. After successfully completing this practice 10 or more times, his mother eventually caught him and decided to sue the City of Livermore for damages related to the content her son was able to obtain at the library. Additionally, Kathleen R. sought to prevent a library from providing Internet access so long as this kind of material was readily available and filters were not firmly in place.⁷⁰

The California Court of Appeals sided strongly with the City of Livermore, explaining that libraries were already facing enough grief from both sides of the Internet filters argument. Section 230 precluded any "provider or user of an interactive computer service" from being "treated as the publisher or speaker" of the information found on that

⁷⁰ Summary derived from *Kathleen R. v. City of Livermore*, 87 Cal. App. 4th 684 (Cal. Ap. 2001).

computer service, and the court proclaimed that a library was also amongst the types of providers which Section 230 was created to protect.⁷¹ This application, the court affirmed, “is fully consistent with the purpose as well as the letter of Section 230.”⁷² Libraries without content filtering systems in place for their Internet networks had officially joined the ranks of AOL, Kinko’s, and Amazon.com.

Section 230, already a force in the area of defamation law, expanded further in the courts to provide immunity for Internet service providers when their users committed other forms of illegal activity on their servers. While the majority of cases discussed up to this point concern defamed individuals, the courts believed it made sense that ISPs and websites should be protected from being liable for other forms of actionable expression. The *Doe* set of cases added sexual predators who engaged in the illegal practice of child pornography or sexual assault against minors to the list of behavior that Section 230 would not allow ISPs and website owners to be held responsible for, once again forcing the injured parties to exclusively seek out and deal with the primary offenders themselves. In the *Livermore* case, a library’s lack of filters may have allowed a minor to download pornography while using their public computers with Internet access, but the courts believed that, like Kinko’s, the library was an Internet service provider. Although Kinko’s is a private business and the library is a public location with free access, the courts pushed Section 230’s boundaries even further by asserting that the lack of filters would not affect the library’s immunity status.

⁷¹ 87 Cal. App. 4th 684, 691 (Cal. Ap. 2001).

⁷² 87 Cal. App. 4th 684, 699 (Cal. Ap. 2001).

At this point in its legal history, Section 230 seems to be an impenetrable force. Yet there are many individuals who have issues with such an unwavering statute governing issues that take place in an industry which is in a constant state of growth and development. In chapter two, the arguments against Section 230 will be unpacked, as well as a list of possible solutions which critics have offered to help reconcile their current issues with this law. This will help shed light on why some of the outcomes of the cases discussed in this chapter may produce troubling legacies, as well as why the Internet has proven to be a somewhat confusing and highly contested medium up to this point.

CHAPTER TWO:
THE INADEQUACIES OF SECTION 230

Brittan Heller and Heidi Iravani were students at Yale Law School, one of the best law schools in the nation. Both women came with honors attached to their name—Phi Beta Kappa, *Yale Law Review*, prestigious internships—yet curiously, neither could secure a job placement during that school year’s on-campus interview proceedings. The idea of having no offers at Yale was relatively unheard of, let alone for students so decorated and hard working. When it came time to sit down and wonder what had gone wrong, though, instead of citing faulty interview skills, the women blamed an outside factor—Autoadmit.com.

At the time, Autoadmit.com was one of the main social networking and online forum websites for law students, lawyers, and those interested in attending law school. Postings on the site’s forums quickly shifted from the topic of law to more private matters and soon the two females became victims of vicious online harassment, misogynistic comments, and accusations about their sexual behavior and health. One poster threatened a sexual assault against one of the women. Another posed as the victim herself giving the impression that she was actively participating in the discussion. Others simply commented on how sexually promiscuous both women were and what kinds of diseases they had contracted due to this promiscuity. It is because of this content that

was made available so freely on the Internet that Heller and Iravani assert employers thought twice about hiring them.¹

The two women sued the website creators for violation of privacy, defamation, and infliction of undue emotional distress, but they were eventually advised to drop the lawsuit against the two male owners.² Their initial lawsuit did, however, allow them to obtain court orders to reveal the identities of the various posters who defamed and harassed them on the website. Since Autoadmit.com did not engage in the practice of IP logging, that is, they did not maintain records of the IP addresses which visited and posted to their site, locating these individuals proved very difficult and only a few were eventually identified. Based on the body of Section 230 casework, it seems that this was the best possible legal outcome the victims could expect. They were rightfully advised to drop the suit against the owners of the website, because the *Schneider* and *Carafano* cases clearly stated that creating a forum for submitting content could not impose liability onto an owner. Furthermore, Autoadmit.com's creators had not over-stepped their role in structuring the forum the way Roommates.com had, and no other exception had been carved out of this seemingly impenetrable Section 230 defense. They were left with only one remedy—find the original offenders and hold them legally and financially responsible for their online behavior.

¹ Ellen Nakashima, “Harsh Words Die Hard on the Web: Law Students Feel Lasting Effects of Anonymous Attacks,” *The Washington Post*, March 7, 2007, Section A.

² Concurring Opinions, “The AutoAdmit Lawsuit,” http://www.concurringopinions.com/archives/2007/06/the_autoadmit_1.html (accessed April 21, 2009).

Regardless of how appropriately their situation played out, though, these two women and countless others who spoke up once the story went public were not satisfied with the results. As students of the law, they found it hard to believe that Section 230 was created by Congress to protect the owners of a website that functioned so that people in the legal community (of all places) could gossip, harass, defame, and insult each other anonymously. While free speech was certainly a principle with strong roots in the Constitution, the fact that it so severely outweighed the right of these victims to obtain justice was also troubling. Autoadmit.com had no legal responsibility to ever remove the postings made about these women, and as a result, their names still constantly came up in search engine results attached to the site. It was also frustrating to recognize that if this information had been published in Yale Law School's newspaper, both the newspaper and the author could have been sued for damages.

All of these are legitimate and relatively consistent criticisms made against Section 230. Although the courts have been very consistent in their interpretation of Section 230, the law has still spurred a great deal of legal research and writing. This is an unusual phenomenon in the realm of legal scholarship. Since Section 230 has been applied so uniformly and produced very little dissent from judges issuing the previously discussed decisions, an individual giving this issue a passing glance would predictably expect that no real legal question or discussion existed in this area of the law. This is not the case with Section 230, and a closer look at the case work that forms the body of this legal issue has produced a great deal of controversy and outcry from students and teachers of the law alike. A review of this scholarship suggests three major problems: first, the courts have misinterpreted the intent of Congress; second, Section 230 is bad

public policy; and third, Section 230 has been applied to create a double standard between the online and print communities.

Criticisms of Section 230

Congressional Intent

The primary and most legally compelling argument against Section 230 stems from the notion that the manner in which it has been so broadly interpreted by the courts is inconsistent with what Congress originally intended when they wrote the law. Brandy Jennifer Glad explains that the “the extent of immunity offered by the courts is in conflict with the language of statute” which removes “any incentive for ISPS to self-regulate the content” and leaves “plaintiffs without an effective remedy.”³ This frustration stems in large part to the fact that the language of Section 230 itself, as with many laws, produces various interpretations. Certain lines are very vague and, depending on an individual’s reading, can produce completely opposite outcomes when analyzing many of the cases discussed in the previous chapter. Section 230 of the Communications Decency Act reads:

(c) Protection for “good samaritan” blocking and screening of offensive material

(1) Treatment of publisher or speaker

³ Brandy Jennifer Glad, “Determining What Constitutes Creation or Development of Content Under the Communications Decency Act,” *Southwestern University Law Review* 34 (2004), 258.

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.

(2) Civil liability

No provider or user of an interactive computer service shall be held liable on account of—

(A) any action voluntarily taken in good faith to restrict access to or availability of material that the provider or user considers to be obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable, whether or not such material is constitutionally protected; or

(B) any action taken to enable or make available to information content providers or others the technical means to restrict access to material described in paragraph (1).⁴

There are two aspects of this language that require immediate further attention before a proper analysis can be conducted. First, the Act goes on to explain that an “interactive computer service” (ICS) as mentioned in line (c)(1) is to be defined 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.⁵

⁴ 47 U.S.C. §230(c).

⁵ 47 U.S.C. §230(f)(2).

An “information content provider” (ICP), which is mentioned towards the end of the same line and again in (2)(B) is defined as “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 [ICS].”⁶ According to these definitions and the overall language of Section 230, an ICS would be granted immunity whereas an ICP, the original author of the message, would not.

Based on these minor clarifications, the first intent based issue which members of the legal community such as Matthew Jeweler have discussed is the application of the term “interactive computer service” to entities beyond traditional ISPs like America Online and Prodigy.⁷ While Glad, Jeweler, and other authors such as Karen Horowitz, Emily Fritts, and Stephanie Blumstein share the sentiment that “providing broad immunity to ISPs where they have exercised traditional editorial functions or merely made information available to others on their services” is consistent with what Congress intended, “following the decision in *Zeran*, courts proceeded to extend immunity beyond those scenarios envisioned by Congress.”⁸ Upon examining the language of the

⁶ 47 U.S.C. §230(f)(3).

⁷ Matthew G. Jeweler, “The Communications Decency Act of 1996: Why Section 230 is Outdated and Publisher Liability for Defamation Should be Reinstated against Internet Service Providers,” *University of Pittsburgh Journal of Technology Law & Policy* 8 (Fall 2007), 19.

⁸ Stephanie Blumstein, “The New Immunity in Cyberspace: the Expanded Reach of the Communications Decency Act to the Libelous ‘Re-Poster,’” *Boston University Journal of*

definition for an ICS, these critics do have cause for complaint. With a strict interpretation, website owners do not seem to be providing access to a computer server or even the Internet for that matter. Common sense would indicate that if a user is visiting the website in question, such as Amazon.com or Myspace.com, then they are already using another provider which has granted them access to the Internet. The argument, therefore, is that perhaps only that primary service provider should be granted immunity rather than the millions of websites that are created every day.

As for the definition of an “Internet content provider” as set forth by the CDA, Horowitz notes that “the threshold where a provider or user of an [ISP] is transformed into an information content provider through the exercise of editorial control” is not explicitly noted, defined, or clarified.⁹ When an ISP becomes “responsible” for creating or developing content, Horowitz explains, is a tough distinction to make, and one that has resulted in questionable court rulings.¹⁰ Roommates.com was considered “responsible” for creating the discriminatory profiles on its website because it limited the answer choices for its users and forced them to answer certain questions about themselves and

Science and Technology Law 9 (Summer 2003); Emily K. Fritts, “Internet Libel and the Communications Decency Act: How the Courts Erroneously Interpreted Congressional Intent with Regard to Liability of Internet Service Providers,” *Kentucky Law Journal* 93 (2004/2005); Glad, 258-259; Karen Alexander Horowitz, “When Is Section 230 Immunity Lost? The Transformation from Website Owner to Information Content Provider,” *Shidler Journal of Law, Commerce & Technology* 3 (Spring 2007); Jeweler.

⁹ Horowitz, 14.

¹⁰ Horowitz, 14.

their beliefs. Yet the Matchmaker website also sought to create a very specific type of content—online dating profiles—and escaped liability simply because it left its prompts open ended and optional. A distinction does exist, but whether or not this is the precise line Congress wished to draw is unknown. Juicy Campus likely would have received protection under Section 230, as well, despite specifically soliciting its visitors for a specific type of information (college gossip) and providing the form and forum to do so. It is quite vexing that these types of websites are not cited for having any role, “in whole or in part,” in regards to the development of their content.¹¹

While the obviously broad or lax interpretation of these definitions has caused a great deal of confusion and aggravation to those who attempt to give Section 230 an in-depth look, the greatest issue related to congressional intent stems from words that are absent from this law. The first line states that “no provider or user of an interactive computer service shall be treated as the publisher or speaker.”¹² Fritts explains in detail why the inclusion of the terms “publisher or speaker” is so crucial, especially considering the term “distributor” was left out.¹³ The distinction between publisher and distributor liability was discussed in the previous chapter’s analysis of *Cubby v. CompuServe*, and as a reminder, publishers are traditionally held more liable for defamation claims than distributors. The only way that a distributor could possibly be held responsible is if it is proven that they were given notice of the offending material and refused to remove it.

¹¹ 47 U.S.C. §230(c).

¹² 47 U.S.C. §230(c).

¹³ Fritts, 778.

Demonstrating that they knowingly allowed the material to continue to exist on their server could make them legally actionable.

Based on this line of thought, Fritts and others have adopted a very dim view of Section 230 and several of its applications.¹⁴ Beginning with *Zeran*, she writes that “AOL was liable as a distributor because it had knowledge of the defamatory material and failed to remove it accordingly.”¹⁵ “Consistent with *Zeran*’s claims,” AOL was notified several times that the postings were defamatory and resulting in harassment, and

¹⁴ Bryan J. Davis, “Untangling the ‘Publisher’ Versus ‘Information Content Provider’ paradox of Section 230: Toward A Rational Application of the Communications Decency Act in Defamation Suits Against Internet Service Providers,” *New Mexico Law Review* 32 (Winter 2002), 75; Neil Fried, “Dodging the Communications Decency Act when Analyzing Libel Liability of On-line Service: *Lunney v. Prodigy* Treats Service Provider like Common Carrier Rather than Address Retroactivity Issue,” *Columbia Science and Technology Law Review* 1 (1999/2000), 1; Keith N. Hylton, “Property Rules, Liability Rules, and Immunity: An Application to Cyberspace,” *Boston University Law Review* 87 (February 2007), 1; Devon Ishii Peterson, “Child Pornography on the Internet: the Effect of Section 230 of the Communication Decency Act of 1996 on Tort recovery for Victims Against Internet Service Providers,” *University of Hawai’i Law Review* 24 (Summer 2002), 763; Barry J. Waldman, “A Unified Approach to Cyber-Libel: Defamation on the Internet, a Suggested Approach,” *Richmond Journal of Law & Technology*, 6 (Fall 1999), 9; Jonathan Zittrain, “Internet Points of Control,” *Boston College Law Review* 44 (March 2003), 653.

¹⁵ Fritts, 776-777.

they still allowed the messages to remain on their bulletin board system.¹⁶ Fritts goes on to explain how this landmark decision paved the way for the several other incorrectly decided Section 230 cases which have mostly continued this trend of confusing publisher liability with distributor liability.¹⁷ In fact, because Section 230 fails to mention distributor immunity explicitly the way it does publisher immunity, Fritts notes that even the *Stratton Oakmont* summary judgment decision, the very case which sparked the creation of Section 230 at the inception of this debate in Congress, is not overturned under the existing language of the law.¹⁸

The *Cubby* court established early on that the publisher versus distributor distinction was a crucial one in the liability debate.¹⁹ Since that case outlined the appropriate standards for determining when an ISP should be held liable, it is puzzling that Congress did not include distributor liability in the language of the CDA. That is, unless that omission was done intentionally. As Fritts explains, “it would be reasonable to surmise that Congress would say ‘distributor’ in addition to ‘publisher’ if it meant ‘distributor’ in addition to ‘publisher.’”²⁰ While the courts have interpreted the statute broadly to include those “entities that would be liable as a publisher of defamatory

¹⁶ Fritts, 776-777.

¹⁷ Fritts, 776-777.

¹⁸ Fritts, 778.

¹⁹ Fritts, 785.

²⁰ Fritts, 778.

material” and “those that would be liable under a distributor liability theory,” it remains unclear whether this application or Fritts’ strict reading of the law is the correct theory.²¹

The final consideration under the congressional intent critique does not delve so much into the actual language of the statute as it does with the history of the law and its creation. Blumstein’s main criticism of Section 230 recalls the Cyberporn Panic and the congressional desire to regulate indecent material on the Internet. Although the *Reno* Court did ultimately strike down the provisions related to the regulation of indecent speech to protect minors using the web, Section 230 was still written in the hopes that it would encourage ISPs to remove this type of material willingly from their servers without having to fear that this type of editorial control would make them liable. Since then, however, the overwhelming majority of cases dealing with Section 230 are related to defamation issues. As Blumstein explains, “few ‘parents are seriously trying to prevent their children from gaining access to defamatory content,’” and it is not the kind of speech that they want the courts to be constantly concerned with.²² Furthermore when their children are in danger because of sexual predators and content on the Internet as in the *Doe* cases, they do not want responsible agencies to shield themselves from taking any sort of responsibility.²³ For a law that was created to help protect minors, Section 230 seems to be doing just the opposite and invoked in cases that have little to do with the matters originally discussed by Congress.

²¹ Jeweler, 18-19.

²² Blumstein, 418.

²³ Blumstein, 418.

Public Policy Argument

When Congress decided to create Section 230, the *Stratton Oakmont* case was still fresh in their minds. Even the possibility that an ISP could be discouraged from exercising editorial control over objectionable content on its network because this would qualify them for publisher liability frightened the individuals working hard to tackle the cyberporn issue. Section 230, they hoped, would provide incentives for ISPs to work with their users and help clean up the Internet. Yet when the *Reno* court struck down the provisions of the CDA that dealt with indecent material, ISPs and other websites were no longer required to remove this type of content when it appeared on their servers. Furthermore, since Section 230 was not one of the provisions challenged by the ACLU, ISPs maintained their immunity status whether they were actively policing their networks or not.

The expansive interpretation of Section 230 by some courts has only worsened this situation. From the *Zeran* case on, the courts have “removed all legal incentives for ISPs, or individuals given ISP protections, to be cognizant of the material they are reposting or to refrain from improper behavior.”²⁴ As more and more cases were lost because an ISP or individual site owner was granted immunity under Section 230, other organizations and websites like them began to recognize that they could maintain a hands-off approach to regulating their site’s content and be free of all legal responsibilities when it came to defamation suits against them. Not only did Section 230 allow them to do nothing, but sites that follow the Juicy Campus model have also used

²⁴ Blumstein, 420.

this immunity to actively encourage posters to make outrageous claims on their website. The success of these websites is based on the idea that users will be willing to gossip about the people they go to school with, live next to, or have dated. When Section 230 is used in this manner, “it is not being used as a shield” from unnecessary litigation, “but as a sword to combat any and all liability for ISPs.”²⁵ Suman Mirmira states that, in essence, the problem today is that although Section 230 “intended to encourage ISPs to self-regulate their content,” it essentially “removed all legal incentives for them to do so.”²⁶ This is why Juicy Campus refused to take down submissions to its website—no matter how hateful or damaging—without an order from the court.²⁷ Legally, they had no obligation to do so. In fact, their only responsibility as business owners was to keep the sight up and functional, leaving them accountable only to themselves.

With this in mind, it is no wonder that companies like Juicy Campus or DontDateHimGirl.com are able “to do whatever they please” with the “free reign,” as Robert Langdon describes it, that they have been granted.²⁸ It seems that the new trend is

²⁵ Fritts, 781.

²⁶ Suman Mirmira, “V. Business Law: 1. Electronic Commerce: a) Internet Service Provider Liability: *Lunney v. Prodigy Services Co.*,” *Berkeley Technology Journal* 15 (2000), 437-438.

²⁷ Juicy Campus, “Privacy & Tracking Policy,” <http://juicycampus.com/posts/privacy-policy> (accessed January 23, 2009).

²⁸ Robert T. Langdon, “The Communication Decency Act Section 230: Make Sense? Or Nonsense?—A Private Person’s Inability to Recover if Defamed In Cyberspace,” *St. John’s Law Review* 73 (Summer 1999), 853.

almost to exploit this immunity, and the type of website Juicy Campus represents has certainly done just that. By basically inviting or, rather, begging Internet users to write unflattering comments about their roommates, fellow classmates, neighbors, ex-boyfriends, and so on, these websites must anticipate that at least some defamation is going to occur. With Section 230, though, what their users may or may not do is of no matter to site owners. As Andrea Julian explains,

By immunizing service providers who have generated at least a minor amount of the offending content... as well as those who either knew or should have known of the defamatory character of the material, Section 230 very nearly encourages reckless dissemination of injurious material. It is, perhaps, too generous to rely on service providers or user to self-regulate when there is no repercussion for failing to do so.²⁹

This explains why websites or service providers that facilitate how information is submitted to them still receive immunity. In the *Carafano* case, Matchmaker.com created a form for its users to fill out which served as the skeleton for the site's online profiles. Even though each profile is submitted to Matchmaker first for approval, signaling that they could have prevented the fake Carafano profile from ever being published on the Internet, Section 230 immunized the Metrospash organization from any class of accountability. When Amazon.com provides a form for its users to submit reviews or Autoadmit.com asks its visitors to provide information about different law

²⁹ Andrea L. Julian, "Freedom of Libel: How an Expansive Interpretation of 47 U.S.C. Section 230 Affects the Defamation Victim in the Ninth Circuit," *Idaho Law Review* 40 (2004), 530.

students, some argue that this sort of facilitation demonstrates a type of control that the site possesses which gives them prior knowledge of the material in question. If these site's have prior knowledge, some legal scholars argue that they should monitor content more closely or be held responsible when things go awry.

“Once it is determined that the defendant is a provider or user of an interactive computer service and that the information was provided by a third party,” Julian writes, “the court will grant immunity regardless of the defendant’s control over or knowledge of the defamatory material.”³⁰ While the *Roommates.com* case demonstrated that at least one court is willing to exert some type of restraint, this instance was certainly an exception to the countless other situations in which Section 230 immunity was deemed appropriate. Most court decisions stem from the fact that “the court will apply an expansive interpretation to the provision that no service provider or user ‘shall be treated as a publisher’ and restrictive interpretation to the definition of ‘information provided by another content provider.’”³¹ That is, they are more than willing to broadly excuse any publisher related activity, such as pre-screening submissions or hiring regular content contributors, but are less willing to veer from the idea that information in any way submitted or created by a third-party automatically excuses an ISP or website owner.

Related to the criticism that ISPs and websites with ISP privileges lack legal incentives to regulate their content is the natural consequence of this fact—“those who are defamed are left without any effective [legal] remedy.”³² A large company can

³⁰ Julian, 528.

³¹ Julian, 528.

³² Glad, 248-249.

assemble their legal team and cover themselves in the blanket of Section 230 immunity, but an average individual has no such resources at their disposal. When a few students at Georgetown University lost their jobs because of claims posted about them on JuicyCampus.com that stated they were drug users and slept with various men, the fact that the website was legally protected from suit and unwilling to remove the offending content from the website left them feeling hopeless and without the proper amount of retribution.³³ The “liberal interpretation,” as Glad calls it, of Section 230 in the courts “has left plaintiffs without an effective remedy.”³⁴ As the definition of an ISP continues to expand and the breadth of what qualifies for immunity broadens further and further into areas many never expected it to protect, the window of opportunity for plaintiffs to recover damages shrinks. This broad interpretation is a “serious injustice” to the “victims of defamatory messages” who unwillingly have false, private information broadcast to millions of individuals over the Internet.³⁵

As if this situation were not already frustrating enough for libel victims, it is often the case that the individual will not only be unable to recover damages from the ISP or website, but the harmful content will also remain untouched or unrevoked from the server. The language of the CDA “specifically indicates that an ISP is not required to do anything—even after receiving notification.”³⁶ David Hallett explains that, under the

³³ “There’s Nothing Juicy About It,” *The Hoya*, September 19, 2008.

³⁴ Glad, 258.

³⁵ Jeweler, 20.

³⁶ David E. Hallett, “How to Destroy a Reputation and Get Away with It—The Communication Decency Act Examined: Do the Policies and Standards Set Out in the

law, they have the option of “[ignoring] any requests or [removing] the material without exposing itself to liability,” no matter how many emails the plaintiff sends or how hard they may try to appeal to the owner(s) emotions.³⁷ These defamed individuals, Matthew Hemmer remarks, “cannot use rights of privacy, defamation, or negligence” to demand that the content in question be removed, or as a foundation to any sort of beliefs that “assurances from the Internet publisher that the [expression] will be removed” will be upheld.³⁸

Some argue that Section 230 does not eliminate all legal options for defamed parties, because the plaintiff still has the option to sue the original creator or poster of the expression in question. Yet even though Section 230 does not excuse the originator of the illegal message, “the creators of the defamatory text are often unknown.”³⁹ “This is exactly the situation Congress created for defamed plaintiffs,” Hallett notes, “A defamed plaintiff has no recourse except to try and find some unknown party who originated the statement.”⁴⁰ This explains why although the option of suing the anonymous poster originally responsible for the message is still available, but this has proved to be

Digital Millennium Copyright Act Provide a Solution for a Person Defamed Online?”

IDEA: The Journal of Law and Technology 41 (2001), 264.

³⁷ Hallett, 264.

³⁸ Matthew D. Hemmer, “Keeping Your Name and Images Private—How Existing Property Law and Requests For Removal Could Stop Unauthorized Display of Your Identity Online,” *Northern Kentucky Law Review* 34 (2007), 735.

³⁹ Glad, 259.

⁴⁰ Hallett, 259.

particularly difficult. After all, website's often boast of their anonymity (Juicy Campus certainly used this feature as a selling point)—no credit card, email address, or other form of identification is required—which means that the only thing linking an individual to his or her message is what is known as an Internet Protocol (IP) address. An IP address is a unique identification number attached to every computer on an online network. Every time that a computer user visits a website, the user's IP address leaves a permanent mark on the website's visitor records almost the way a passport gets stamped at every new location.⁴¹ While websites like Juicy Campus can not reveal the names of its online posters (presumably because they do not collect or maintain this type of information), they could provide the IP address of the offending poster which would allow defamed parties to locate the computer of origin and sue its owner. In a situation where the victim feels that they have a strong defamation suit against an anonymous poster, however, a court order must still be obtained in order to force a website like Juicy Campus to reveal such identifying information.⁴²

Obtaining a court order of this nature can often be a tedious process, and sometimes even an IP address offers little to no information regarding the identity of the speaker. For example, if the person posting defamatory statements over the Internet uses a public computer found in a library, school, or other public location, the IP address could link the offending message to a computer but not a specific user. It would be up to the location to maintain completely reliable and accurate records in order for the victim to

⁴¹ Juicy Campus, "Privacy & Tracking Policy."

⁴² What is my IP address? "My IP address," [http:// www.ip-address.com/](http://www.ip-address.com/) (accessed March 27, 2009).

avoid reaching a dead end in their pursuit of justice. No case serves as a better example of this predicament than the *Kinko's* incident. Since the Kinko's store was a publicly accessible location where any patron could pay to use their online services and they did not maintain records of individuals who visited their store, the victim was unable to identify the person who wronged them. The computer user left no traceable information—they paid for the services in cash—and Kinko's was granted immunity, so the PatentWizard name was left without remedy in this instance. Furthermore, several websites are currently available which actually allow Internet users to “cloak” or disaggregate their IP address from their Internet usage. These IP-cloaking websites can be easily found with a quick Google search (www.Internetcloak.com and www.anonymizer.com are two of the most popular Internet cloaking websites), and they make it almost impossible to identify speakers of defamatory statements.⁴³ At one point while it was still a functioning website, Juicy Campus even encouraged their users to use these types of programs by advertising their existence in the “Frequently Asked Questions” section of their site.⁴⁴

With all of these road blocks in place, it is no wonder that some members of the legal community fear that, “in the absence of indirect intermediary liability, significant harms will go undeterred or unremedied,” particularly the justice that affected parties

⁴³ Google, “IP Cloaking Search,”

<http://www.google.com/search?hl=en&q=ip+cloaking&btnG=Search> (accessed March 27, 2009).

⁴⁴ Juicy Campus, “Frequently Asked Questions (FAQs),”

<http://juicycampus.com/posts/frequently-asked-questions> (accessed January 23, 2009).

seek and deserve.⁴⁵ Legal scholars such as Cara Ottenweller, Ryan Savage, David Wiener, and Scot Wilson fear that Section 230 immunity has crossed over into dangerous territory with little concern for the victims it leaves in its wake.⁴⁶

Plaintiffs in these actions may find themselves in a situation where the individual who originally supplied the material cannot be identified, the Internet disseminator cannot be sued, and there is no right to demand that the materials be taken down or to rely on assurances that they will be taken down.⁴⁷

This passage paints a very grim picture for victims of online defamation, but the cases that have been discussed previously clearly demonstrate that it is not an unreasonable or inaccurate picture to paint. As anonymous postings become the more common form of online user contribution, the lack of legal incentives provided to ISPs presents a growing

⁴⁵ H. Brian Holland, "In Defense of Online Intermediary Immunity: Facilitating Communities of Modified Exceptionalism," *The University of Kansas Law Review* 56 (January 2008), 393.

⁴⁶ See Cara J. Ottenweller, "Cyberbullying: The Interactive Playground Cries for a Clarification of the Communications Decency Act," *Valparaiso University Law Review* 41 (Spring 2007), 1285; Ryan Savage, "Between a Rock and a Hard Place: Defamation and Internet Service Providers," *Asper Review of International Business and Trade Law* 2 (2002), 107; David Wiener, "Negligent Publication of Statement Posted on Electronic Bulletin Boards: Is There Any Liability Left After *Zeran*?" *Santa Clara Law Review* 39 (1999), 905; Scot Wilson, "Corporate Criticism on the Internet: The Fine Line Between Anonymous Speech and Cybersmear," *Pepperdine Law Review* 29 (2002), 533.

⁴⁷ Hemmer, 734.

problem is the realm of defamation prosecution. Congress may have felt that Section 230 was necessary to allow the Internet to grow and flourish and to promote the free flowing of ideas over the web, but the provisions of the CDA do not take into account that “maintaining the free marketplace of ideas” should not come “without a cost, that is, compensation to the defamed plaintiff.”⁴⁸

Double Standard

The final issue that critics have addressed in regards to Section 230 is the double standard it creates between print and online publishing. While both the print and online worlds possess similar fundamental qualities—both have authors providing content for a large group of readers—their libel cases are handled quite differently. As Ryan King mentions, under Section 230, “the service provider may select and publish a defamatory statement made by another party and may refuse to remove the statement from its service even after it knows that the statement is false.”⁴⁹ Online service providers can essentially publish third-party content without the burden of wondering whether or not the information they are providing is accurate or breaks any laws. Even if they do have additional knowledge about the expression in question, they are not obligated to take any action without the courts express order to do so and ultimately will not be held

⁴⁸ Julian, 533.

⁴⁹ Ryan W. King, “Online Defamation: Bringing the Communications Decency Act of 1996 in Line with Sound Public Policy,” *Duke Law & Technology Review* 2003 (October 6, 2003), 24.

responsible. Newspapers, magazines, and other “traditional providers” are subject to the “common law” standards that were mentioned briefly in the introduction of the first chapter.⁵⁰ In order to prove that defamation has occurred in the non-cyber world, those filing a suit must prove that the message in question (1) can be perceived as harmful or insulting; (2) has been heard, read or viewed by a third party; (3) clearly identifies the person being defamed; and (4) demonstrates actual malice if the person is a public figure or mere negligence if the individual is a private person.⁵¹ Michelle Kane notes that, once a plaintiff proves that these four conditions have been met, “common law courts [impose] strict liability” against the publisher “with no need for a finding of fault.”⁵² A judge could even award damages to the plaintiff, Kane clarifies, without the defamed individual “proving any actual harm to [his or her] reputation.”⁵³ While these common law standards exist and proving defamation is still no easy task, they are a far cry from the sweeping and automatic immunity of Section 230. A traditional provider will always be held liable “if it publishes or distributes defamatory material,” King notes, regardless of who was the original creator of the message.⁵⁴ This is why these traditional typed of publications spend a great deal of their resources checking (and double checking) sources

⁵⁰ King, 24.

⁵¹ Thomas L. Tedford and Dale A. Herbeck, *Freedom of Speech in the United States*, 5th ed. (State College, Pa: Strata, 2005), 82-83.

⁵² Michelle J. Kane, “1. Electronic Commerce: b) Internet Service Provider Liability: *Blumenthal v. Drudge*,” *Berkeley Technology Law Journal* 14 (1999), 485.

⁵³ Kane, 485.

⁵⁴ King, 24.

or asking for comments from both sides of an argument. They have a vested journalistic—and monetary—interest in making absolutely sure that the information they publish does not qualify as libel.

This discrepancy between how cases are handled when they occur in the real world versus the cyber world is particularly troublesome when examining cases involving newspapers or magazines that also have an online component or version of their publication. David Myers, a professor at the Valparaiso University School of Law, cites a story related to him by a colleague at *The Washington Post* as an example. When the newspaper published a defamatory story, he explained, it was “liable for that product.”⁵⁵ When the same story appeared on their website, washingtontpost.com, however, the case went nowhere and “the company [was not] liable under Section 230 of the CDA.”⁵⁶ This was one story published by the same company—the only difference was the medium used to transmit that story to the mass population—and yet the legal challenges produced two very different outcomes. With this type of system in place, a newspaper or magazine could simply reserve its controversial or questionable stories for the online version of its newspaper to ensure it is never prosecuted for defamation. As the online news world continues to grow—most, if not all publications have thriving and frequently updated

⁵⁵ Joshua Azriel, “The California Supreme Court’s decision in *Barrett v. Rosenthal*: How the Court’s Decisions Could Further Hamper Efforts to Restrict Defamation on the Internet,” *Hastings Communications and Entertainment Law Journal* 30 (Fall 2007), 94-95.

⁵⁶ Azriel, 95.

websites—this contradiction could present some rather troubling results for injured parties.

Blumenthal v. Drudge also sheds serious light on the double standard issue. This case presents a “fundamental unfairness” because the court “allows AOL to benefit from Drudge’s attraction, yet bear no burden for his carelessness.”⁵⁷ Blumenthal could sue the *Drudge Report*, but he could not sue AOL for widely disseminating the same story to its subscribers who had paid a fee much like those who subscribe to publications like *The Washington Post*. Even though AOL hired Drudge and willingly published his column as a part of their member services, the court felt that they should not be held in any way responsible thanks to the protection of Section 230. The *Blumenthal* court “let AOL get away with actions that would never be tolerated in any other medium,” and they did so under the guise of the CDA.⁵⁸ The courts are almost empowering service providers like AOL to do as they please knowing that ultimately, if something should go awry, there is another person who will receive all of the blame. If the blamed party is ultimately not punished either, then service providers can still relax knowing that any sort of responsibility has been deflected on to another individual who the plaintiff can choose to be angry at. Drudge ultimately emerged unscathed by the Sydney Blumenthal incident, but he could have easily been found liable in a court of law. Who knows if AOL would have been there to support him if the situation would have had that kind of outcome, especially after their own conscience had been wiped clean by the judge.

⁵⁷ Kane, 501.

⁵⁸ Kane, 501.

Similarly, traditional libel law states that a person who “carelessly or recklessly” re-posts or circulates defamatory statements “may be just as guilty as the libel’s author.”⁵⁹ *Batzel v. Smith* and *Barrett v. Rosenthal*, two cases that deal with the re-posting or redistributing of defamatory content, illustrate that the same standard does not apply on the world-wide-web. Even though “repeating a false statement can injure a person’s reputation to the same, or even higher, degree as did the original statement,” only the primary creator of the defamatory content can be held responsible on the Internet.⁶⁰ Kane continues to shed light on this issue by clarifying that online defamatory statements are “also instantaneous” and “more pervasive than statements made on television or in the newspaper,” but since some do not consider [them] as “permanent as ‘ink on dead trees,’” the court treats them uniquely.⁶¹ While traditional newspapers and magazines require an individual to wait for a printing press and the mail carrier to access stories that may feature this type of content, the Internet is updated constantly and known for its second-by-second accuracy. While a person has to pay for a newspaper or magazine, an online connection makes all of this information available for free and straight from the home or office. The fact that re-posting is acceptable on the Internet is precisely the reason why Internet bloggers such as Perez Hilton, an infamous celebrity gossip columnist who updates stories on perezhilton.com almost to the minute that they occur, can link to or re-post the contents of false or salacious news stories found on other celebrity gossip blogs or online tabloids without a second thought to the possible

⁵⁹ Blumstein, 407.

⁶⁰ Blumstein, 407.

⁶¹ Kane, 501.

consequences. If the content qualifies as defamation, then its original author will be held responsible, and Perez Hilton can simply move on to the next headline and reap the benefits of the increased online traffic which the controversial story may bring to his site. Perez Hilton is one of the more popular examples of individuals who make a living re-posting this kind of content over the Internet, but in reality he is one of thousands. When all of these sites continuously re-post a particularly newsworthy or attention grabbing incident, it makes it almost impossible to kill the story and make the problems that it causes the defamed individual go away.

These double standards have many wondering why the courts feel that the Internet is so unique or special. If anything, critics argue, in today's society the Internet is far more pervasive than both print and radio, and as such defamation that occurs online could reach far more people and result in serious damage to the reputation of an affected individual. Jae Jong Lee agrees and explains how the Internet, like print and broadcasting, is responsible for "the transmission of vast quantities of information," and is "probably not so unique as to require the formulation of a truly novel approach to defamation liability."⁶² Radio broadcasters once "proposed broad immunity from defamation liability for third-party content, an idea that resembles 230 immunity," but they are obviously denied this privilege to this day.⁶³ If radio should be denied such a

⁶² Jae Hong Lee, "Batzel v. Smith & Barrett v. Rosenthal: Defamation Liability for Third-party Content on the Internet," *Berkeley Technology Law Journal* 19 (2004), 488.

⁶³ Lee, 488.

license, then it remains to be seen why the Internet should still be granted such a vigorous “full measure of First Amendment protection.”⁶⁴

This is a fact which has left many legal scholars quite disconcerted.⁶⁵ Kane writes that, “all members of society deserve some protection against unwarranted attacks on their reputations regardless of whether such attacks are made on paper or in cyberspace.” The medium should not determine whether or not someone’s grievances are addressed. Back when newspapers first emerged as a form of mass media communication, it was forecasted that “the widespread circulation of newspapers presented increased power for doing injury to reputations,” and this warning is still relevant in the context of the Internet. The Internet has already far surpassed newspapers in its potential as a mass media tool, and as such should have certain legal protections in place for those who “may be damaged by careless citizens of cyberspace.”⁶⁶ Regulation of the Internet, or a lack

⁶⁴ *Reno v. American Civil Liberties Union*, 521 U.S. 844, 880 (1997).

⁶⁵ See Sewali K. Patel, “Immunizing Internet Service Providers for Third-Party Internet Defamation Claims: How Far Should Courts Go?” *Vanderbilt Law Review* 55 (March 2002), 647; David V. Richards, “Posting Personal Information on the Internet: A Case for Changing the Legal Regime Created by Section 230 of the Communications Decency Act,” *Texas Law Review* 85 (April 2007), 1321; Melissa A. Troiano, “The New Journalism? Why Traditional Defamation Laws Should Apply to Internet Blogs,” *American University Law Review* 55 (June 2006), 1447; Andrew J. Slitt, “The Anonymous Publisher: Defamation on the Internet After *Reno v. American Civil Liberties Union* and *Zeran v. America Online*,” *Connecticut Law Review* 31 (Fall 1998), 389.

⁶⁶ Kane, 501.

thereof, is “based on an outdated policy decision” which may need to be reexamined in order to reconcile the apparent discrepancies between the online and print worlds.⁶⁷

Some attribute this double standard to the fact that the Internet is still “in its infancy.”⁶⁸ These critics hold the belief that Section 230 is a temporary piece of legislature that will be done away with or amended once the state of the Internet becomes more stable and law makers are more aware of what direction it is headed in. The Internet is no longer “in its infancy,” though, and would probably better be described at this point in its history as a “vigorous and muscular adolescent.”⁶⁹ Perhaps it is time that Section 230 is reexamined under the context that common law principles are in effect and full force in all other mass communication mediums.

Proposed Solutions

A review of the legal scholarship criticizing Section 230 would not be complete without the solutions that have been suggested to combat the problems it poses. Once again, three main lines have been identified as areas which have been given the most attention by critics. These proposed solutions include (1) establishing levels of editorial or some other identifiable control that could induce liability; (2) adopting notice and take down provisions modeled after the Digital Millennium Copyright Act, the current statute that governs online copyright and trademark infringement and dilution; or (3) repealing

⁶⁷ King, 24.

⁶⁸ Lee, 491.

⁶⁹ Lee, 491.

Section 230 completely and reverting back to the traditional publisher-distributor distinctions which currently govern real world defamation suits and were employed in the early online cases such as *Cubby*.

Establish Levels of Control

When Section 230 was enacted, it still remained to be seen how exactly the courts would apply the statute to various members of the online community. Internet service providers (ISPs) were quickly protected via *Zeran*, and this was an expected conclusion considering AOL constituted what had traditionally been considered an ISP. The company, like CompuServe and Prodigy before it, was merely providing access to the Internet and supplying no additional original content to its subscribers. When Section 230 expanded to include Internet content providers (ICPs), who not only provided traditional service but some original content for their users to view and respond to, the law was pushed further into previously uncharted areas of the web. Still further, the final category of online companies and websites, the Internet content facilitators (ICFs), received Section 230 immunity and seemed to possess even more power and control over the original content on their websites and how users could contribute their own forms of expression.

At the time that the two women filed their lawsuit against the creators and owners of Autoadmit.com, very little was known about the role that those two gentlemen played in the website's maintenance and organization. It is possible that with the several hundred posts that are made on their website each day, they had no prior knowledge that

such conversations were taking place on their server. Therefore, it can be argued that these men had no control over the situation or the behavior of their users. Conversely, however, as an ICF, AutoAdmit.com could have reasonably predicted that the format and nature of their website would encourage these types of postings and make them easily available to other users. It could be claimed that the operators chose to create a forum for members of the law community and actively controlled the manner in which these postings were expressed. This idea of having “control”—who has it and to what extent do they exercise it—has become a crucial component in the discussion regarding Section 230 reform.⁷⁰

According to the definitions set forth in Section 230, an Internet provider could lose its immunity if it is found responsible, “in whole or in part,” for creating or

⁷⁰ See also Anthony Ciolli, “Blogger as Public Figures,” *The Boston University Public Interest Law Journal* 16 (Spring 2007), 255; Eric Danowitz, “Myspace Invasion: Privacy Rights, Libel, and Liability,” *Journal of Juvenile Law* 28 (2007), 30; Joseph Dowling, “*Noah v. AOL Time Warner*: Are There Legitimate Barriers to Civil Rights Protection on the Internet?” *Albany Law Journal of Science & Technology* 14 (2004), 775; Eric Goldman, “Bloggership: How Blogs Are Transforming Legal Scholarship,” *Washington University Law Review* 84 (2006), 1169; Theodore George, “Censoring Internet Access at Public Libraries: First Amendment Restrictions,” *Boston University Journal of Science and Technology Law* 5 (Spring 1999), 11; Lyrissa Barnett Lidsky, “Silencing John Doe: Defamation and Discourse in Cyberspace,” *Duke Law Journal* 49 (February 2000), 855; Aaron Perzanowski, “Relative Access to Corrective Speech: A New Test for Requiring Actual Malice,” *California Law Review* 94 (May 2006), 833.

developing information on the Internet.⁷¹ Glad writes that the first step to establishing whether an “ISP helped to create or develop content” is to “look to the extent of control the ISP exercised over the text.”⁷² The easiest way to establish a level of control is to return to the publishing aspect of running an Internet service provider or website and review the company’s editorial policies. Glad and other critics are right to acknowledge that Section 230 was created to provide immunity for ISPs when “traditional” editorial control takes place.⁷³ There are limitations, however, and this should not be an invitation to exert any kind of editorial functions without being held responsible for these actions. To begin, Glad highlights that the when “editorial control is conferred immunity under Section 230,” there is presumption that the “‘form and message’ of the content” will not change.⁷⁴ If an ISP chooses to edit the message and meaning or form in which it was originally expressed is somehow altered, Glad ascribes that immunity should not be granted.

Others feel that this interpretation does not go far enough. As Barry Waldman suggests, actively editing statements made by other users should always result in liability.⁷⁵ He explained that this suggestion is in accordance with the original intent of the CDA because “once the ISP takes an active editing role it becomes the ‘co-author’

⁷¹ 47 U.S.C. §230(f)(3).

⁷² Glad, 26.

⁷³ Glad, 96.

⁷⁴ Glad, 96.

⁷⁵ Waldman, 9.

and falls outside the CDA protection.”⁷⁶ Waldman claims that the statute’s requirement that ISPs act in ““good faith”” is violated if something like a defamatory statement on Autoadmit.com goes through an editorial process and the editors still choose to publish it.⁷⁷ Andrea Julian agrees, and she strongly advocates that the “blanket immunity problem” could be solved if ISPs are no longer granted immunity in these situations where it is obvious that someone at the company “knew or should have known of the defamatory nature of the material and had the power to control its dissemination.”⁷⁸ These critics base their suggestions on the idea that if someone is reading these posts either in advance or at some other point in the publishing process, that individual should make an honest effort to screen the content which is obviously objectionable. Leaving it on the Internet so that it can be read several times over and spread throughout the web is negligent and should therefore be punished with a lack of immunity.

With respects to control, another school of thought which has arisen deals more with the actual creation or development of material rather than just the editing that material goes through. The statute claim’s that creating or developing “in whole or in part” can force immunity to be taken away, but this has not been the case in every circumstance.⁷⁹ “Allowing immunity for someone like an [ICP] who provides some, though not all, of the content” is not consistent with this language and seems to violate

⁷⁶ Waldman, 9.

⁷⁷ Waldman, 9.

⁷⁸ Julian, 511.

⁷⁹ 47 U.S.C. §230(f)(3).

the original intent of the statute.⁸⁰ For example, if in the *Drudge* case AOL had contributed its own content, no matter how significant, to Matt Drudge's columns, immunity would not have been granted to the ICP.⁸¹ This new rule would not require AOL to create the column completely on its own, but simply contribute any part of the form in which the column is finally expressed to the public. Now, it may be easier to identify when an ICP or website has contributed any kind of actual content, large or small, to a finished product, but legal scholars have reminded their readers that developing content is also cause for losing immunity.

“Control,” as Davis explains, “encompasses control over the ultimate shape and destiny of the final product.”⁸² He compares the role of an ISP or website owner to that of a director, and he explains that “the director of a movie might not contribute any dialogue, set design, or other tangible elements to a film; however, directors are often considered co-authors of movies in which they exert ultimate control over the shape of the final product.”⁸³ This is what Glad refers to as “facilitation,” a concept which relates directly back to Julian's notion that prior knowledge could lose an ISP or website its immunity rights.⁸⁴ With this new standard and the existence of ICFs in mind, the decision in the *Roommates.com* case seems reasonable—posing specific questions to users and forcing them to answer with a limited number of responses denotes an obvious

⁸⁰ Glad, 263.

⁸¹ Davis, 95-96.

⁸² Davis, 96.

⁸³ Davis, 96.

⁸⁴ Glad, 263.

role in developing the final product of the user's profile. However, under this interpretation, the Matchmaker website from the *Carafano* case would not have fared so well. An argument could be made that Matchmaker's decision to structure their profiles with specific areas for their users to add pictures, write about themselves, list hobbies, and state preferences constitutes at least partial development of their content.

Also, websites like JuicyCampus.com, DontDateHimGirl.com, and AutoAdmit.com could be considered facilitators under Glad and Julian's standards because based on the goals their websites set forth at their creation, they should have had a reasonable and almost definite expectation that defamation was going to occur on their server. A website like DontDateHimGirl.com which asks its readers to submit information about men who other women should stay away from romantically must anticipate that not every user is going to be honest, accurate, or shy away from unflattering embellishments. Since the owners of this website possess the power necessary to control the dissemination of this information, this solution suggests that increased liability should be one of the expected hazards when creating such a website. While the degree to which these standards should be applied seems to vary among legal critics, their arguments suggest that examining the "extent and quality" of control which ISPs and websites possess and exert is a viable solution to the conundrum that Section 230 has created.⁸⁵ Whether this control constitutes creation or development of the content on Internet servers is an issue which the courts have not addressed properly up to this point.

⁸⁵ Glad, 262.

Impose Notice and Take Down Requirements

While a discussion of what constitutes editorial control and creating or developing content is beneficial, the scholarship in this area is still in its early stages of development, and legal scholars do not seem to have come to a clear consensus on what exactly this type of reform would entail.⁸⁶ Conversely, several authors have endorsed a policy which is quite clear in its intent and scope. This is because their proposal for improving Section 230 involves modeling an existing statute: the Digital Millennium Copyright Act (DMCA). The DMCA is like the CDA in that it “protects service providers from liability for content provided by third parties,” but it also stipulates one crucial differing component.⁸⁷ In order to receive immunity under the DMCA, an ISP is required “to act”

⁸⁶ See also Paul Ehrlich, “Regulating Conduct on the Internet: Communications Decency Act Section 230,” *Berkeley Technology Law Journal* 17 (2002), 401; “*Grace v. Ebay, Inc.*” *Berkeley Technology Law Journal* 20 (2005), 335; Ryan Lex, “Can Myspace Turn Into My Lawsuit?: The Application of Defamatory Law to Online Social Networks,” *Loyola of Los Angeles Entertainment Law Review* 28 (2007/2008), 47; Doug Lichtman and Eric Posner, “Holding Internet Service Providers Accountable,” *Supreme Court Economic Review* 14 (2006), 221; James D. Shanahan, “Rethinking the Communications Decency Act: Eliminating Statutory Protections of Discriminatory Housing Advertisements on the Internet,” *Federal Communications Law Journal* 60 (December 2007), 135; Sean P. Trende, “Defamation, Anti-SLAPP Legislation, and the Blogosphere: New Solutions for an Old Problem,” *Duquesne Law Review* 44 (Summer 2006), 607.

⁸⁷ Julian, 532.

in order to escape liability for copyright infringement allegedly taking place on its network.⁸⁸ This call to action most directly revolves around take-down and put-back provisions outlined in the DMCA.

The provision which legal scholars seeking this remedy have chosen to focus on is the notice and take-down procedure outlined by the DMCA. This procedure is simplified by King:

Upon receiving a valid notification, the service provider retains its immunity if it adheres to a set of formal procedures. The service provider must first inform the party that provided the [content] that the [content] will be removed from the service. The service provider is only required to take reasonable steps to contact the content provider, such as, sending an email to the address that was connected to the original posting. The content provider may submit a counter notice declaring that the [content is not illegal]. If he or she submits a counter notice, the service provider must put the disputed [content] back onto the interactive computer service within ten to fourteen business days. The injured party may then seek an injunction declaring that the [content is illegally being used] and that it must be removed. The service provider is not involved in the court proceedings, but must comply with the order.⁸⁹

While Congress would have to be “specific on what a notice shall contain,” such a specific and well-structured process would “[alleviate] responsibility from the ISP.”⁹⁰

⁸⁸ Hallett, 266.

⁸⁹ King, 28.

⁹⁰ Hallett, 267-268.

Instead of making difficult judgment calls as to what kind of content control would constitute a “good faith” effort under the CDA, ISPs “would simply follow the process laid out.”⁹¹ This shift, critics argue, would be as easy as “[changing] the CDA to encompass all of the notice and counter notification requirements” in the DMCA, and many agree that it is the simple solution Congress has been ignoring for years.⁹²

As Lee describes, revising Section 230 in the manner could “restore some of the balance” currently lacking between “fostering the growth of the Internet, encouraging self-regulation of undesirable content, and protecting individuals from the harm of defamation.”⁹³ Under a DMCA modeled version of Section 230, an ISP could be held liable if (1) it had actual knowledge that a statement is defamatory; (2) had knowledge of facts which make the defamatory nature of a statement obvious; (3) received financial benefit directly from a defamatory statement; or (4) was notified that a statement is defamatory and did not remove the statement from its service as outlined in the aforementioned guidelines.⁹⁴ King further clarifies that a DMCA-like policy would allow the ISP to sue an individual for “expenses incurred” if their claim turned out to be

⁹¹ Hallett, 268.

⁹² Hallett, 267; See also Mark A. Lemley, “Digital Rights Management: Rationalizing Internet Safe Harbors,” *Journal on Telecommunications & High Technology Law* 6 (Fall 2007), 101; Olivera Medenica and Kaiser Wahab, “Does Liability Enhance Credibility?: Lessons from the DMCA Applied to Online Defamation,” *Cardozo Arts & Entertainment Law Journal* 25 (2007), 237.

⁹³ Lee, 493.

⁹⁴ King, 27.

fraudulent.⁹⁵ Since this new policy is based on clarity and detailed instructions, King goes on to note that an allegedly defamed individual should consider the ISP notified only when “a formal written notification” has been submitted to the ISP.⁹⁶

For example, imagine that a man named Walter dates a woman named Alice. After a difficult relationship and subsequent break-up, Alice posts that Walter is “has Chlamydia and his business, Company X, is on the verge of bankruptcy.” Walter notifies DontDateHimGirl.com, the website in question, formally in writing that the posts are untrue and that he will sue if they are not removed. Under the new DMCA modeled version of Section 230, DontDateHimGirl.com would be required to remove the posting or face possible liability if the statement did in fact turn out to be defamatory. They would then notify Alice that the statement had been removed, and she would have the option to respond with a request that the post be reinstated if she felt that no defamation had occurred. If in fact the statement turned out to be true and Walter’s company was in fact filing for bankruptcy or treating a sexually transmitted disease, not only would Alice’s posting return to DontDateHimGirl.com’s website, but the website operators could potentially sue Walter for any fees they incurred as a result of responding to his claim.

At least one legal scholar, Suman Mirmira, calls for reform that goes beyond the DMCA. Continuing the theme that the CDA and Internet provisions in general should be very specific and well-structured, Mirmira proposes a records-based initiative. While his suggestions are not included in the original language of the DMCA, they fit into the

⁹⁵ King, 27.

⁹⁶ King, 27.

overall structure of the statute because maintaining records seems to be a logical requirement in order to notify posters when their content is removed from a website. This records-based initiative would entail users providing “a name and either a credit card or driver’s license number to the [ISP] who would then verify the information.”⁹⁷ Citing the widespread anonymity available on the Internet as an issue, Mirmira explains that keeping these records would allow any posting to be traced back to its author so that the author can be notified when it is removed or held legally responsible if necessary. While he agrees that this practice may seem “burdensome” and to “violate individual users’ privacy,” Mirmira maintains that this is “by and large the existing practice.”⁹⁸ Most ISPs currently charge their users fees to use the Internet and set up accounts, and several websites require visitors to sign-in or set up accounts using personal information, email addresses, and passwords as a means of identifying new visitors. In the past, Mirmira explains, such ISP or website maintained content “has been used to identify users indulging in Internet-related criminal activities” and to make sure that they face the appropriate legal penalty.⁹⁹

What Mirmira is proposing is that these commonly implemented practices become law. He writes that ISPs and websites “have a duty to maintain accurate records of user identities and activities” so that they can be called upon by the courts when necessary.¹⁰⁰ This all relates back to the “good faith” effort proscribed in Section 230.

⁹⁷ Mirmira, 454.

⁹⁸ Mirmira, 454.

⁹⁹ Mirmira, 454.

¹⁰⁰ Mirmira, 455.

To Mirmira, this is such an important promise that ISPs make to their users that when they fail, either accidentally or purposely, they should make every effort to repair the relationship. Although other authors mentioned it in passing, Mirmira is the only critic who included that ISPs should post a retraction when “any message [is] proven to be defamatory.”¹⁰¹ Although not an escape hatch by any means, he feels that this act “would compensate the plaintiff at least partially for the damage done to his reputation.”¹⁰²

Mirmira’s additions notwithstanding, up to this point it is widely speculated that this mechanism has not been adopted because it creates an “unreasonable burden” for ISPs and website operators.¹⁰³ Yet as Blumstein describes the situation, “with respect to defamation, Congress and the courts have concluded that requiring ISPs to self-regulate is overly burdensome, yet when it comes to copyright and trademark infringement, that same burden is tolerable.”¹⁰⁴ These authors hold that adopting a DMCA-like policy would not be “unrealistic or impossible” and would entail a simple responsibility “varying according to the size of the bulletin board.”¹⁰⁵ While trademark and copyright law is decidedly different from the world of defamation litigation, supporters of this solution advocate that they could be governed “equally well” by the same procedure.¹⁰⁶

¹⁰¹ Mirmira, 455.

¹⁰² Mirmira, 455.

¹⁰³ Blumstein, 425.

¹⁰⁴ Blumstein, 426.

¹⁰⁵ Blumstein, 425.

¹⁰⁶ Blumstein, 425.

Repeal Section 230

Despite these suggested alterations to the existing interpretation or language of Section 230, there are still some critics who believe that the best solution is to repeal Section 230 completely. Citing the noted Supreme Court Justice Oliver Wendell Holmes, best known for his famous dissents, Robert T. Langdon explains why striking the statute down is paramount.

The ‘puke test’ is allegedly Justice Holmes’s way of deciding whether or not a statute ought to pass constitutional muster. Essentially the ‘puke test’ says, ‘a statute or other act of government violates the Constitution if and only if it makes one want to throw up.’ A person who has been degraded, trampled, chastised, morally wronged, and stigmatized by defamatory statements over the Internet and is precluded from recovery in a court of law might want to ‘puke’ in reference to Section 230.¹⁰⁷

Keeping with this theme, most critics in favor of eliminating Section 230 use the public policy arguments described previously to support their call for action. Legal scholars like Jeweler strongly believe that Section 230 “works a serious injustice on the victims of defamatory messages posted on the Internet,” and that there are ways to reconcile the interests of both ISPs and defamed parties.¹⁰⁸ An overwhelming majority of the critics who suggested that Congress should repeal Section 230 recommended that traditional tort principles should be applied to the Internet. This requires returning to the traditional

¹⁰⁷ Langdon, 853.

¹⁰⁸ Jeweler, 20.

publisher-distributor distinction set forth in *Cubby*—the standard which is applied to real world defamation issues. This solution would eliminate the double standard problem that currently plagues the print and online news worlds and would give victims of defamation more adequate legal resources.

Adopting this “common law framework” would allow courts to “decide on a case-by-case basis what common law category a given ISP falls into based on its role and function” in each particular situation.¹⁰⁹ This means that an issue “arising out of an ISP’s publisher functions,” such as in the *Stratton Oakmont* case where an Internet service provider actively edited its content to meet its service agreements, would involve applying the standards which traditional publishers such as Random House and print newspapers abide by.¹¹⁰ If service provider’s “distributor functions” are the root of the problem, an event that could likely occur if an Internet content provider like AOL hired Matt Drudge to provide outside content or a financial company to assemble its stock portfolio information, real world distributor standards commonly applied to libraries, bookstores, and newsstands should be the norm.¹¹¹ If the ISP is simply fulfilling its duty as a “common carrier” by transmitting electronic mail, instant messages, or other online private messages, a situation that could be envisioned in the case of some of the Internet content facilitators who provide the forums for individuals to submit messages and

¹⁰⁹ Jeweler, 21.

¹¹⁰ Brian C. McManus, “Rethinking Defamation Liability for Internet Service Providers,” *Suffolk University Law Review* 35 (2001), 669.

¹¹¹ McManus, 669.

dictate how these messages are distributed, then the most analogous real world standards could possibly be those set forth for telephone companies.¹¹²

Supporters of this policy find it advantageous for a number of reasons. Due to the fact that they believe that Section 230 “has been interpreted more broadly than Congress intended,” returning to the standard used before its creation could help correct some of the wrongs that have been committed by the courts since its inception.¹¹³ As Fritts asserts, “the Communications Decency Act was meant to overrule *Stratton Oakmont* [not] *Cubby*,” and therefore the “publisher/distributor distinction must continue to be used in defamation analysis for individual reputations to receive the protection they deserve.”¹¹⁴ Section 230 removed all incentives for ISPs to monitor their servers and police content, both advantages Congress originally sought to benefit from, and re-implementing the existing real world standard would give ISPs the motivation necessary to “prevent and respond to instances of cyber-defamation.”¹¹⁵ Moreover, when Section 230 was created, Congress and other supporters of the law believed that it was necessary to promote the growth of the Internet, a seemingly new and poorly understood mass media tool. Yet the Internet has grown so rapidly that Section 230 and their original rationale “carries much less weight today.”¹¹⁶ Its growth is so rapid that to this day, its limits, power, and scope are still relatively unknown or properly understood. Until the

¹¹² McManus, 669.

¹¹³ Jeweler, 21.

¹¹⁴ Fritts, 784.

¹¹⁵ McManus, 669.

¹¹⁶ Jeweler, 21.

Internet becomes more stable and a law which accurately reflects its role in mass media communication is written, supporters of Section 230's extermination believe that the traditional laws which have served other forms of communication well up to this point should be employed. Any other option at this point, one critic notes, is "simply irrational and illogical."¹¹⁷

Despite his use of a description of Holmes's "puke test," Langdon does concede that Section 230 would possibly pass constitutional scrutiny in the Supreme Court. The Court could stand by the idea that it is unreasonable to expect major ISPs to monitor every single bit of content which is submitted and respond in a timely fashion to legal claims made by users. Plus, without Section 230, it is possible that the vast number of defamation lawsuits could flood the court system and cripple these Internet businesses. Yet while he acknowledges that there are some "minimally rational" explanations for why Section 230 is necessary, Langdon does not accept that the statute "should remain on the books."¹¹⁸ "There can be no doubt that Internet providers need to assume some responsibility for the material that pass through their services," he writes, and he and his fellow authors deem the "distributor framework" to be the "most logical solution."¹¹⁹ He concludes by stating that Congress now has three tasks—to rethink, abolish, and return. They must "rethink the impact of Section 230" on the online defamation landscape, "abolish it," and "return" to a system which never needed fixing.¹²⁰ The publisher-

¹¹⁷ Langdon, 855.

¹¹⁸ Langdon 853.

¹¹⁹ Langdon, 855.

¹²⁰ Langdon, 853.

distributor distinction, as well as various other traditional legal standards, is the answer to what these critics consider bad law.

In the previous chapter, it became evident that Section 230 was a reliable source of immunity for Internet service providers, content providers, and content facilitators alike. Yet despite this consistency in the court room, it is also not without its faults. The three major issues that legal scholars seem to have with Section 230 are its veer from perceived Congressional intent, public policy issues, and the double standard it creates between online and print publications. These criticisms are not without their solutions, however, and there is a great deal of legal scholarship which suggests that regulating levels of editorial control, adopting a DMCA modeled formula, or repealing Section 230 altogether in favor of traditional tort principles may be the answer to the perceived flaws of the statute. In the final chapter, the solutions provided will be strictly scrutinized in order to determine whether they best fulfill the role of solving the problem plaguing online defamation and its victims. Based on this analysis, a new standard for evaluating this type of speech and subsequent Section 230 based immunity will be offered. This solution will specifically bear in mind the growing prevalence of Internet content facilitators such as Juicy Campus who have used the privilege of this immunity to evolve the way websites function and collect content from their users. Section 230 does not balance the interests of the Internet's operators and users well enough as it stands, and a new approach to legislation in this area must recognize that as the Internet continues to grow and expand into new areas, the new issues that emerge must also be addressed.

CHAPTER THREE:
A RESPONSE TO THE SECTION 230 DEBATE

Juicy Campus may have gone out of business due to lack of funding in early 2009, but the elimination of a single website does not solve one of the current issues facing the Internet today.¹ As an Internet content facilitator, Juicy Campus was merely a member of a much larger class of websites which are springing up all over the web and changing the way users communicate with one another. There is virtually a new site for every kind of gripe or area of gossip an individual would need to pursue—ex-lovers, neighbors, classmates, teachers, family members, roommates, employers, authors, doctors, and so many other groups have fallen victim to the formula which ICFs have created. Rather than simply using Section 230 as an excuse to adopt lax editorial and regulatory policies regarding the content on their websites, these companies have taken the abuse of Section 230 immunity a step further. Websites such as RateMyProfessors.com, MyExGF.com, and CollegeACB.com have actually created forums which encourage users to post defamatory and other types of privacy violating content and given them the mechanism to do so anonymously. Knowing that they are guaranteed immunity no matter what their users choose to say or do, these websites invite salacious behavior and the amount of traffic and revenue it brings to their sites.

Acknowledging the new issues that these websites present, it seems that it is time to reevaluate Section 230 and amend it in some form. After close examination of

¹ Carrie Thornton, “New Gossip Web Sites Follow in Wake of JuicyCampus.com,” *The Daily Toreador*, March 6, 2009.

the solutions proposed in the previous chapter, however, it seems that most critics have been misguided in their attempts at reform. While a greater balance is necessary in the ongoing power struggle between online service providers or website owners and those individuals who are wrongfully affected by forms of expression found on their servers, establishing levels of control, imposing notice and take down requirements, or repealing the statute all together are not the most effective ways to handle the Section 230 problem.

Answering the Proposed Solutions

Establishing Control Levels Is Unworkable

Punishing a website for the degree of editorial control it exercises creates its own set of issues and discrepancies. Jennifer Glad is right to concede that, for some service providers and website owners, it would be nearly impossible to sift through the hundreds or thousands of posts that are made on a daily basis on their networks.² Such a task would involve hiring more employees and developing a thorough coding mechanism for determining which posts should be eliminated or altered and which can remain on the server. Furthermore, such a mechanism would privilege large companies capable of making such additions to their staff, whereas smaller or newer companies with fewer

² Brandy Jennifer Glad, “Determining What Constitutes Creation or Development of Content Under the Communications Decency Act,” *Southwestern University Law Review* 34 (2004), 263.

employees and resources would simply not be able to match the man-power and efficiency of their larger competitors.

If Barry Waldman's belief that actively editing statements made by other users should always result in liability is to be proscribed to, then the original intent of Congress is completely missed.³ When the Cyberporn Panic broke out in the mid-90s, Congress feared that the *Stratton Oakmont* decision would discourage ISPs from taking an active role in policing the content on their networks. The immunity from liability for third-party content was enacted expressly so that companies like CompuServe, Prodigy, and American Online could determine the type of content they wanted on their servers and eliminate content which they felt violated their terms and policies. Fulfilling this role should not make an ISP or website a "co-author" of the material in question.⁴ Considering that one of the largest criticisms against Section 230 is that it gives those receiving immunity no incentives to screen or edit content, it seems troubling that Waldman advocates on behalf of punishing them for actually performing the opposite.

Furthermore, Waldman and Andrea Julian claim that the Section 230 problem can be solved if ISPs are no longer granted immunity when it is apparent that a member of the organization's staff "knew or should have known of the defamatory nature of the

³ Barry J. Waldman, "A Unified Approach to Cyber-Libel: Defamation on the Internet, a Suggested Approach," *Richmond Journal of Law & Technology*, 6 (Fall 1999), 9.

⁴ David E. Hallett, "How to Destroy a Reputation and Get Away with It—The Communication Decency Act Examined: Do the Policies and Standards Set Out in the Digital Millennium Copyright Act Provide a Solution for a Person Defamed Online?" *IDEA: The Journal of Law and Technology* 41 (2001), 259.

material and had the power to control its dissemination.”⁵ Unless the individual is a public figure involved in a high-coverage, newsworthy event, it seems impossible to affirmatively prove how an employee could know if the content in question is in fact defamatory. Seeing as how the ISP or website would have no prior knowledge or relationship with the victim, determining whether a statement made about that individual is true or false is not viable. Someone may write on a website like Juicy Campus that “Sandra Lee steals regularly from the office that she works for,” but such a claim would be difficult to verify considering there may be hundreds of Sandra Lee’s working in hundreds of offices at hundreds of college campuses around the nation. Expecting a reader to determine the defamatory nature of a statement at face value is a burdensome request and would undoubtedly create a chilling effect on the Internet. If these companies are held liable for statements that they “should have known” were defamatory, their policy could very well shift to one that involves eliminating any content which is controversial, overly critical, or likely to be disputed.⁶

Likening an Internet service or content provider to “the director of a movie,” as Bryan Davis does, because these organizations “exert ultimate control over the shape of the final product” is also an unfair distinction to impose.⁷ Of course these business

⁵ Andrea L. Julian, “Freedom of Libel: How an Expansive Interpretation of 47 U.S.C. Section 230 Affects the Defamation Victim in the Ninth Circuit,” *Idaho Law Review* 40 (2004), 511.

⁶ Julian, 511.

⁷ Bryan J. Davis, “Untangling the ‘Publisher’ Versus ‘Information Content Provider’ paradox of Section 230: Toward A Rational Application of the Communications Decency

owners are going to “exert ultimate control over the shape of the final product” of their business—this is a function arguably performed by all good business owners with a vested interest in the success of their company and the use of their brand.⁸ A movie director spends months or years devoted to the completion and perfection of a single project, whereas Internet companies are arguably involved in thousands of stories at a time. Expecting a website operator to perform director-like duties for every message posted to its Internet server creates a chaotic situation and prevents these individuals from properly carrying out their roles as business owners. While Glad mentions “facilitation” as the term which should govern this area of reform, even this concept can be applied to the normal functions of several companies.⁹ As Jonathan Friedman and Francis Buono explain, while not all companies “prescreen content” several, including AOL, “aggressively monitor [their] chat areas, message boards, and other services for defamatory or otherwise offensive content.”¹⁰ This is because these companies have “community standards” which they enforce should a user choose to breach these previously agreed upon conditions.¹¹ In a way, by performing these tasks and others like

Act in Defamation Suits Against Internet Service Providers,” *New Mexico Law Review* 32 (Winter 2002), 96.

⁸ Davis, 96.

⁹ Glad, 263.

¹⁰ Jonathan A. Friedman and Francis M. Buono, “Limiting Tort Liability for Online Third-party Content Under Section 230 of the Communications Act,” *Federal Communications Law Journal* 52 (May 2000), 664.

¹¹ Friedman and Buono, 664.

it, companies like AOL are facilitating the type of image they wish to portray to their users and other observers. This is not a punishable offense, and ISPs and websites should be encouraged to facilitate these results and set these predetermined expectations for their users to positively impact the content being disseminated online.

It may seem advantageous to develop a scheme for determining when exercising control over content crosses the line of immunity and into liable territory, but such requests are underdeveloped, poorly defined, and overly burdensome to Internet operators as they stand. The statute has already come under fire for its vagueness and overly broad interpretation, and the language employed by the advocates of this solution does little to solve this issue. By presenting those who control the status of the online world with such a burdensome and sometimes impossible task, Glad, Waldman, Julian, and Davis do not further the goals of the Internet nor do they increase the protection available to injured parties. Perhaps if the definitions and distinctions they preview are further advanced and the issues mentioned previously are taken under consideration, such a scheme could be reexamined for further consideration. As it stands, though, the solution involving the control scheme does not fit in with the current state of the Internet, especially with regards to the Juicy Campus brand of Internet content facilitators at the heart of this reform.

Notice and Take Down Requirements Are Flawed

Applying the standards of the Digital Millennium Copyright Act may seem like a simple and well outlined solution. The policies of the DMCA and its notice and take

down provisions are adequately defined and well structured. However, it is interesting and somewhat confusing that Ryan King, David Hallett, Suman Mirmira, and Stephanie Blumstein would advocate on behalf of adopting a policy which does not function correctly even for its originally intended area of law.¹² As it stands, the DMCA is not the ideal model for addressing copyright and trademark issues on the Internet, and it has been the subject of its own criticism and calls for reform.¹³ The DMCA has created three main issues for websites that are sometimes used to illegally distribute copyrighted works: (1) these websites are often bombarded with take down notices; (2) the desire to avoid legal liability often leads to the removal of legitimate content; and (3) the re-posting of content in violation of the statute is widespread and uncontrollable.¹⁴

Notice-based initiatives lead to ISPs and websites being bombarded by claims that infringement or dilution has occurred on their network. While this may be an easy task

¹² See Stephanie Blumstein, "The New Immunity in Cyberspace: the Expanded Reach of the Communications Decency Act to the Libelous 'Re-Poster,'" *Boston University Journal of Science and Technology Law* 9 (Summer 2003), 418; Hallett, 259; Ryan W. King, "Online Defamation: Bringing the Communications Decency Act of 1996 in Line with Sound Public Policy," *Duke Law & Technology Review* 2003 (October 6, 2003), 24; Suman Mirmira, "V. Business Law: 1. Electronic Commerce: a) Internet Service Provider Liability: *Lunney v. Prodigy Services Co.*," *Berkeley Technology Journal* 15 (2000), 437.

¹³ Matt Jackson, "The Digital Millennium Copyright Act of 1998: A Proposed Amendment to Accommodate Free Speech," *Communication Law and Policy* 5 (Winter 2000), 61.

¹⁴ Jackson, 78-92.

for a website that only receives a few hundred posts or less in a week, companies like facebook.com and AOL would be faced with the possibility that the millions of users who use their services every day could be engaging in activities that would result in a notification from another user or an outside party. What will result is that these companies will eventually cease reading the contents of these notifications and simply take down any flagged material regardless of whether the claim is legitimate at face value or not. While creating a parody which uses clips from a song or movie does not violate copyright law—legitimate parodies are considered a fair use—if the movie studio or record company that owns the rights to the film or recording dislike the use of their content in this manner, they could file a complaint with the website. If a huge company like Amazon or Myspace.com actually finds the time to read the notification statements of these companies in their entirety, they may overlook the studio or record label's lack of understanding of copyright law in favor of simply removing the material and hoping that they can be spared of any further correspondence or legal entanglements regarding the matter.

Such a predicament poses an obvious threat to free expression on the Internet. While the original author could issue a counter-complaint to have the message reinstated, the provisions outlined in the previous chapter state that an ISP could take up to two weeks to do so. This is unacceptable when it is considered that the message in question could have a sense of timeliness attached to its overall impact. While the example of a parody may seem a bit trivial, a user could also be posting information that is important or newsworthy. For example, imagine that a customer had a legitimate complaint or opinion regarding a scene in a film or a singer or rapper's choice of lyrics. This

individual may wish to voice their complaint or observations in the form of a video blog or recording or broadcast an online radio show and maintain a copy of the program's voice feed on the Internet for users to listen to. If in this video or broadcast the individual chooses to use scenes or dialogue from the movie or audio clips of the song to enhance the quality of his argument by providing concrete evidence, the studio or record label could once again issue complaints and have the speech silenced. While the postings may very well be returned to their original location after fourteen days, they could now be lost in the countless other postings that have been published since then. While the intricacies of their arguments could take far longer than fourteen days to unfold, it seems unsettling that such important information and other content like it could be in limbo for two weeks during which active measures to solve the problem or increased dialogue about the issue could have been carried out.

The same could be said about an issue involving defamation law. While stating that "Jimmy is an idiot" or "Susan is a bitch" is not considered defamation since it can be construed as the opinion of the poster—neither statement is fact-based—Jimmy or Susan may not like these statements and file a complaint with the website. Rather than assessing the merits of their claims and explaining the nature of defamation on the Internet, the website would likely remove the statements. On a more serious note, imagine if the Watergate scandal would have taken place with today's available technology. If Deep Throat had chosen to leak the details of the incident that ultimately led to the termination of several government employees and the resignation of President Nixon in an online political message board, under this model, nothing would have prevented the White House from challenging these claims and having them removed

before the story could catch on. During political elections a similar form of censorship could easily occur if, for example, President Barack Obama had hired interns to patrol the web for unflattering content about his campaign and subsequently asked them to file a defamation suit that all of this information could be removed from the web. Presently, there are also many websites in existence which serve as “gripe sites.” That is, they are websites that were created by consumers to protest or expose their grievances against various products, industries, organizations, or public figures. Two of these sites include Screw-PayPal.com, which the author states was created to expose the online payment company PayPal “for what it is: a den of thieves,” and OrlandoFloridaSucks.com, an anti-tourism website created by an Orlando, Florida resident.¹⁵ If the DMCA modeled provisions were applied to defamation law, PayPal and the Orlando Tourism Bureau could easily file a defamation claim to eliminate these unflattering websites from the Internet.

Supporters may counter that in the previously mentioned examples, if the situation was so serious and time sensitive the user could simply re-post the message which would require the allegedly infringed upon party to file a second complaint. This concept of re-posting to counter every take-down resulting from notifications provides a solution to individuals whose content is being wrongfully censored, but it also presents a grave problem for persons or groups whose copyrights and trademarks are actually being abused and diluted. If in the time it takes someone to notify an ISP that copyright

¹⁵ Orlando Florida Sucks, “Home,” <http://www.orlandofloridasucks.com/> (accessed April 28, 2009); Screw PayPal, “About ScrewPayPal.com,” <http://www.screw-paypal.com/about.html> (accessed April 28, 2009).

infringement has occurred the original author of the message can re-post his content as many times as he wishes, the original purpose of the notification scheme has been defeated. In fact, the original author's message could even be copied by other users and reprinted on various websites or bulletin boards, forcing the victim to notify more than one company. While the DMCA does stipulate that at some point repeat offenders must be removed from the server and stripped of their privileges to use the network or website, depending on the ISP or website's registration process, an individual can often create as many accounts as he or she wishes.¹⁶ There is also no definition as to what constitutes the "appropriate circumstances" in which an account would need to be terminated in the first place.¹⁷

In fact, the video hosting website YouTube.com is currently entangled in a \$1 billion lawsuit brought against them by media powerhouse Viacom for these very problems. Viacom claims that while YouTube does comply with the DMCA, it sometimes removes content too slowly. The way YouTube's services are set up, material that is removed is often quickly re-posted by several users and multiple accounts can easily be used to the infringer's advantage. While the courts have yet to rule on the matter of *Viacom v. YouTube.com*, it remains to be seen whether the provisions of the DMCA can be reconciled with the growing power of the Internet. Indeed, some companies are so overwhelmed by the YouTube effect that they have simply brokered deals with the popular website or created their own accounts and channels on the

¹⁶ 112 Stat. 2860 (1998).

¹⁷ 112 Stat. 2860 (1998).

YouTube network.¹⁸ Since the popularity of the website has grown so quickly, these companies determined that it was a shrewd business decision to control their own online content in at least some form. Meanwhile, YouTube itself has admitted that when they receive a notification, the user is immediately notified and the material is removed from their server.¹⁹ Users, including the infamous celebrity blogger Perez Hilton, have complained that their original content, which did not violate any copyright or trademark laws, has been incorrectly removed from YouTube due to false or overzealous copyright holder complaints.²⁰

As far as Suman Mirmira's addition to this discussion is concerned, his suggestions are also flawed. It seems ideal to be able to constantly maintain accurate

¹⁸ Summary derived from Online Media Daily, "Copyright Lawsuit Allowed to Proceed against YouTube," http://www.mediapost.com/publications/?fa=Articles.showArticle&art_aid=104652 (accessed April 27, 2009); CNET News, "Google to Publishers: We're Not Evil or Illegal," http://news.cnet.com/8301-1023_3-10213903-93.html (accessed April 27, 2009).

¹⁹ YouTube, "Community Guidelines," http://www.youtube.com/t/community_guidelines (accessed April 28, 2009); You Tube, "Copyright Notices," http://www.youtube.com/t/dmca_policy (accessed April 28, 2009).

²⁰ Perez Hilton, "About the YouTube Bullshiz...", <http://perezhilton.com/2007-12-21-about-the-youtube-bullshiz> (accessed April 28, 2009); Perez Hilton, "Dear YouTube," <http://perezhilton.com/2007-12-18-dear-youtube> (accessed April 28, 2009); Perez Hilton, "YouTube Is Censoring Us!!!!!!" <http://perezhilton.com/2007-12-18-youtube-is-censoring-us> (accessed April 28, 2009).

records of users and their activities on the Internet, but this is simply impossible. Not only is it feasible and common for users to provide false information, but this practice is unreasonably burdensome to both the operator of the server and the user. Internet users visit such a vast number of websites that it seems unnecessary to have them register with every interactive service or website that they visit. Having to verify this information is simply another hurdle in the way of these ISPs and website owners running their companies and ensuring smooth and reliable service for their users. Furthermore, it is entirely possible that this information could be appropriately verified and still misidentify the individual seeking access. Children, for one, have been known to use their parents' credit cards and other personal information to gain access to content on the Internet, and professional hackers engage in identity theft practices for this very purpose. Plus, with all of the available software and other services that allow users to travel the Internet undetected, those who wish to break the law and not be caught still have access to all of the resources they would require to do so.

Mirmira's addition that retractions should be a mandatory addition to the standards governing this area of the law, while slightly unrelated to the overall DMCA model, are also worth some discussion. While it is true that companies like YouTube post messages that content has been removed for violating their terms and conditions on their website for users to view when they try to access previously removed material, a retraction policy would do little to advance the interests of defamation victims.²¹ As Jennifer Liebman discusses, "the nature of the Internet" forces these retractions to carry very little effect and weight. If the purpose of the retraction is to "cause the speaker

²¹ YouTube.

inconvenience and financial hardship,” then the online world’s “low barriers to entry” eliminate any great effort or costs on the part of the issuer of the apology.²² If the intent is to eliminate or ease the impact or prevalence of the message on the Internet, then a retraction is also an ineffective method because “it is very easy to preserve [online speech] permanently.”²³ With re-posting and search engines alone, any content once made available on the Internet can still be found, as Liebman notes, by “those who know where to look.”²⁴

While the intent behind a DMCA modeled notice and take down scheme was rooted in solving the problems plaguing Section 230, it seems to provide no such solution. Unfortunately, the circumstances involving the current state of the DMCA’s effectiveness with regards to copyright and trademark clearly demonstrate that its adoption to the world of online defamation issues would not go as smoothly as enthusiasts such as King, Hallett, and Blumstein describe. One statute faced with criticism and concern can not be fixed by being replaced with another statute riddled with similarly crippling issues. The goal of a law should partly involve decreasing the amount of unnecessary litigation and paper work that could flood Internet providers or servers and the courts alike, and this model advances no such interest.

²² Jennifer Meredith Liebman, “Defamed by a Blogger: Legal Protections, Self-Regulation and Other Failures,” *University of Illinois Journal of Law, Technology & Policy* 2006 (Fall 2006), 368.

²³ Liebman, 368.

²⁴ Liebman, 368.

In Defense of Section 230

The final solution which is offered by Robert Langdon, Matthew Jeweler, and Brian McManus asserts that the only way to effectively deal with Section 230 is to repeal the law and revert to the traditional tort principles that were employed by the courts before the law's creation.²⁵ This proposed policy change is an exaggeration which does not serve the involved parties in this debate in the best possible manner. As Jon Burns describes, the broad immunity which Section 230 has provided websites allows and “[facilitates] free user expression.”²⁶ This broad interpretation, Burns notes, is consistent with the “express will of Congress—to promote a healthy exchange of ideas with minimum government regulation—and with the realities of the Internet today, which now services over one billion people.”²⁷

²⁵ Matthew G. Jeweler, “The Communications Decency Act of 1996: Why Section 230 is Outdated and Publisher Liability for Defamation Should be Reinstated Against Internet Service Providers,” *University of Pittsburgh Journal of Technology Law & Policy* 8 (Fall 2007), 19; Robert T. Langdon, “The Communication Decency Act Section 230: Make Sense? Or Nonsense?—A Private Person’s Inability to Recover if Defamed In Cyberspace,” *St. John’s Law Review* 73 (Summer 1999), 855; Brian C. McManus, “Rethinking Defamation Liability for Internet Service Providers,” *Suffolk University Law Review* 35 (2001), 669.

²⁶ Jon Burns, “*Doe v. SexSearch.com*: Placing Real-Life Liability Back Where It Belongs in a Virtual World,” *North Carolina Journal of Law & Technology* 9 (Fall 2007), 85-86.

²⁷ Burns, 86.

While this solution would solve the existing double standard between the online and print media and put more power in the hands of defamed individuals, it would also weigh down the court system and adversely affect the development of the Internet. Jeweler notes that under this format, courts would be able to “decide on a case-by-case basis what common law category a given ISP falls into based on its role and function” in each particular situation.²⁸ While Jeweler writes this as if it were an advantage, having to evaluate online defamation suits in such an open, unique, and individual manner presents an onerous task for judges and juries alike. If the Internet, with its unparalleled amount of users and contributors were to adopt real world defamation standards, the courts would also be inundated with an endless amount of lawsuits which would undoubtedly slow down the effectiveness of the legal system and properly serve neither party. If it took years for one lawsuit to make its way to a judge after waiting behind thousands of claims just like it, it may not be worth the financial resources spent to try to recover damages or have the content removed since such a long period of time has elapsed. Victims would have more adequate legal remedies, but at the cost of wasting an indefinite amount of time, money, and energy with no guaranteed results.

Moreover, the Internet is simply not the same kind of mass media tool as the television, radio, or newspaper. It is impossible to fully liken activities performed on the Internet to that of television or radio stations, publishing houses, or book stores because it presents a new opportunity for users which no other medium has been able to match. The Internet’s “low barriers to entry”—the opportunity it provides any person to speak and

²⁸ Jeweler, 21.

say whatever they choose—is unique to it alone.²⁹ The scarcity of available stations prevents most members of society from contributing to television and radio broadcasts and other content disseminated over the airwaves. Newspapers are comprised of hired staff members whose work goes through a thorough editing process before it is printed for subscribers to read. While members of the public have the opportunity and are encouraged to submit their content in the form of letters to the editor and op-ed pieces, these contributions are also subject to editing and only a very limited selection of submissions are chosen for publication.

The Internet allows anyone to become a part of the conversation whenever they choose to do so. For the first time ever, any person, so long as they have online access, can become a journalist, a radio talk show host, an author, or a news anchor. While *The New York Times* has about 1300 people in its newsroom, the Internet has over one billion people from all over the world contributing to the stories that are being told on its network.³⁰ This quality makes the Internet so unique and novel that it simply can not be governed by the same traditional principles that these forms of expression are subject to. Repealing Section 230, a statute that ensures the continued growth of this powerful medium and protects service providers and websites from the unpredictable behavior of these one billion individuals, would cripple the status of the Internet. It is not, as Langdon accuses, “irrational and illogical” to expect that holding the Internet to the same standards as a much smaller and not so expansive mass media tool would hinder its

²⁹ Liebman, 368.

³⁰ Richard Perez-Pena, “*New York Times* Plans to Cut 100 Newsroom Jobs,” *The New York Times*, February 14, 2008.

growth and development and force certain online companies and websites to shut down.³¹ While newspapers may face a manageable number (if any) of defamation suits annually, a large website could encounter thousands and spend an expectedly large and possibly business-ending sum on legal fees and settlements. Newspapers devote entire divisions of their offices and plenty of time prior to publication to the editing process presumably to preempt these types of incidents, and once again the size and nature of the Internet prevents it from developing such a luxury.

Also, it should be noted that with the arrival of Internet content facilitators, a special brand of website has begun to leave its mark on the Internet. McManus attempts to analogize various forms of Internet companies to real world counterparts—he compares the *Stratton Oakmont*-deemed publisher, Prodigy, to Random House and AOL's distribution of the *Drudge Report* to a bookstore—but his analogy fails when he compares these ICFs to telephone companies.³² Their programming structure is much more complicated, and it involves the creation of a specialized forum, third-party content, additional user comments, and sometimes even ratings systems. Essentially these websites are providing their users with a network to contribute their content, their own original content in the form of the website's intended purpose and mission statement, and the ability to engage in conversations with their peers through the use of additional comments, private messages, and awarded ratings. They also often facilitate this activity in a manner in which their users can remain anonymous. With all of these factors in play,

³¹ Langdon, 855.

³² McManus, 669.

it is difficult to find a real world match whose standards could be similarly employed to this complex online counterpart.

Langdon asserts that service providers and websites “need to assume some responsibility” for the behavior of their users and the illegal, defamatory statements that these companies post on their networks.³³ Whether Langdon’s assertion is to be interpreted as true or not, this responsibility can not take the form of a publisher-distributor model. While Section 230 has provided a great deal of controversy surrounding various public policy issues, the needs and rights of injured parties can not be advanced in this case without severely hindering the ability of the majority to speak freely in a manner which no other medium allows them to do.

Section 230, as it stands, provides a valuable and necessary resource for the rapidly growing adolescent that is the Internet. Although it has been subject to a great deal of scrutiny, its consistent application by the courts to grant immunity to Internet service providers, Internet content providers, and Internet content facilitators alike demonstrates what a crucial component it is to that continued development. Despite this consistency, however, it does seem that the statute provides a chance for improvement so that the interests of these valuable providers can be balanced with those users who are wronged by third-party contributors. With the growing popularity of Internet content facilitators particularly in mind, now more than ever the opportunity for reform must be seized. Unfortunately most of the solutions that have been offered at this point in the discussion of the statute seem inadequate and unable to properly solve the dilemma. While levels of editorial and other forms of control is a topic often raised in the Section

³³ Langdon, 855.

230 debate, such a formula has been poorly defined up to this point and would impose an overly burdensome and impossible task on those responsible for regulating the Internet. A solution modeled on the notice and take down provisions of the DMCA is not the appropriate way to deal with Internet content facilitators. Repealing Section 230 altogether and adopting traditional tort principles to govern the Internet would rigorously impede the progress made by this technological innovation and flood the legal system with defamation actions. An analysis of the flaws contained in these proposed solutions has led to the conclusion that Section 230 is a necessary and valuable statute which is fundamental to furthering first amendment interests on the Internet. However, there is a selection of solutions which have not been discussed up to this point which could give victims a form of redress while this immunity is maintained, even in a post-Juicy Campus Internet.

Social Changes

While the issue of Section 230's broadened immunity has sparked concern and criticism, it is possible that the threat Internet content facilitators pose could take care of itself. For this to occur, various social changes already in development would have to continue to grow and be adopted by individuals using the Internet. When Juicy Campus shut down in early February of 2009, its creator, Matt Ivestor cited a lack of "online ad revenue" and "venture capital funding" as the reason for its demise.³⁴ Ivestor blamed the

³⁴ Mark Millian, "Juicy Campus Shuts Down, Kills the College Grapevine," *Los Angeles Times*, February 4, 2009, Technology.

“historically difficult economic times” for the lack of available resources, but when *US News & World Report* ran the story, visitors to the publication’s website commented that this lack of ad revenue was likely due to the site’s controversial nature.³⁵ One user stated, “Who would want their ads running next to hate-filled and slanderous messages that ruin people’s lives?”³⁶ This commenter raises a valid point. Juicy Campus proved to be so controversial and generally disliked by its target audience—college students—that it could no longer financially sustain itself and was seemingly forced to shut down by the market. Its replacement, CollegeACB.com, is very similar to Juicy Campus, but it has not caught on with the public or the media the way its predecessor did. CollegeACB.com receives considerably less visitor traffic, and among those visitors, the majority does not post original content to the site the way users did on Juicy Campus.³⁷

These facts seem to imply that if a website like Juicy Campus really does have no place on the Internet, eventually it will force its own demise. Websites, like most businesses, are governed by market forces and consumer need. If consumers decide that they have no need for Juicy Campus or other websites like it, advertisers will reflect that

³⁵ Heather Mayer, “Juicy Campus Shut Down,” *The Daily Orange*, February 5, 2009, News.

³⁶ *U.S. News & World Report*, “Juicy Campus Will Be Shut Down,” <http://www.usnews.com/blogs/paper-trail/2009/02/04/juicy-campus-will-be-shut-down/comments/2> (accessed April 30, 2009).

³⁷ Alexa, “JuicyCampus.com vs. CollegeACB.com,” <http://www.alexa.com/siteinfo/juicycampus.com+collegeacb.com> (accessed April 30, 2009).

attitude and refuse to do business with the site. An Internet data assembly site indicates that while Juicy Campus' popularity spiked during its first few months on the web in early 2008, a period marked by most of its media coverage, its traffic continued to decrease every month following this time.³⁸ Without the popularity it once enjoyed, its owners and employees had nothing to offer other companies in exchange for their necessary ad dollars. One of the major lessons learned from the Juicy Campus debacle seems to be that if an individual does not like the nature or business of a website, then they should simply stop going to the site and encourage others to boycott it as well. Since most websites do not charge visitors to read or submit content, profits are often based solely on advertising revenue, and since companies want their ads to be seen by the largest amount of potential consumers possible, every visit to an Internet content facilitator has value.

In addition to the implications of Juicy Campus's demise, there is also something to be said for developing a greater amount of cyber-literacy before visiting these websites. A few incidents indicate that progress is already being made in the area of cyber-literacy. When the social networking website Facebook first emerged on the web, college students eagerly joined its network, and the site's membership grew exponentially each month.³⁹ On the website, individuals posted various personal facts about themselves including names, college majors, cell phone numbers, addresses, and hobbies and also uploaded thousands of pictures to the site's mainframe. All of this information was

³⁸ Alexa.

³⁹ Alexa, "Facebook.com," <http://www.alex.com/siteinfo/facebook.com> (accessed April 30, 2009).

completely available to users and visitors of the Facebook website alike, and soon companies began hiring employees whose job it was to patrol the Internet and visit websites like Facebook and its predecessor Myspace.com to look for photos or content that should preempt them from hiring students.⁴⁰ Similarly, many universities began using Facebook as a tool for dealing with pre-planned on-campus parties and discovering students who had engaged in underage drinking and posted photos online.⁴¹ When word got out that companies and schools were engaging in these types of practices, students were left stunned.⁴² For once, they had no one to blame but themselves, because the material on Facebook was completely self-reported and self-submitted.

In response to the growing concern regarding student job prospects and school sanctions, Facebook adopted stricter privacy settings which many of its users took immediate advantage of. Today, many students have barred their profiles from public viewing and been much more selective when accepting friend requests which would grant other users access to their private information and photos. In 2009 when Facebook attempted to change its privacy policy to include a provision that would give their company ownership and ultimate control over the dissemination of all of the material posted to its website, users opposed it so vehemently and threatened to leave the social networking program with such conviction that it abandoned the new format almost

⁴⁰ Amy S. Clark, "Employers Look At Facebook, Too," *CBS News*, June 20, 2006.

⁴¹ Janhavi Purohit, "Some Schools Look to Facebook, Myspace," *The Triangle*, September 26, 2008.

⁴² Marina Agapakis, "Facebook.com a Danger to Students Seeking Employment," *The Dartmouth*, April 11, 2006.

immediately until it could come up with a policy that was more user friendly.⁴³ Since then, Facebook has asked its users to vote on the policy amendments they approve and feel best protect their privacy rights on the Internet.⁴⁴ In the context of Internet content facilitators, this greater awareness surrounding privacy issues on the Internet could signify that users would be less likely to post content on such public forums. While these websites encourage visitors to post information about other people, users may begin to realize that the person being victimized could easily be themselves or that posting a hurtful or defamatory statement would encourage retaliation from the victim in a manner which would come back to harm the original poster.

Another trend seems to indicate that while these incidents involving defamatory postings are somewhat embarrassing and undesirable, they may not have the consequences once imagined. In January of 2009, Olympian Michael Phelps was caught smoking marijuana from a glass bong.⁴⁵ As a national hero, the incident instantly made headlines and incited media frenzy.⁴⁶ Yet as the coverage went on, more and more

⁴³ Chris Walters, "Facebook's New Terms of Service: 'We Can Do Anything We Want With Your Content. Forever,'" *The Consumerist*, February 15, 2009.

⁴⁴ Facebook, "Privacy," <http://www.facebook.com/home.php> (accessed April 30, 2009); Scott Duke Harris, "Facebook Users Vote for 'Bill of Rights,'" *Mercury News*, April 24, 2009; Dani Neuharth-Keusch, "Controversial Changes to Facebook's Terms of Service Put to Vote," *The Cornell Daily Sun*, April 28, 2009.

⁴⁵ Tim Perone, "Michael Phelps Caught With Bong," *New York Post*, January 31, 2009.

⁴⁶ Mike Celizic, "Phelps: 'It Was a Bad Mistake,'" *The Today Show*, March 13, 2009; Georgina Dickinson, "14-Times Olympic Gold Medal Winner Michael Phelps Caught

people came out in defense of the gold-medalist, and the results of an online poll seemed to indicate that most Americans did not have their opinions about Phelps changed as a result of the incident.⁴⁷ *Saturday Night Live* cast member Seth Meyers dedicated an entire segment of the February 7, 2009 episode to berating (albeit humorously) the media for turning the story into such a controversy, when, in his opinion, nothing worthy of punishment or public shaming had occurred.⁴⁸ In an editorial piece written for *The Heights*, it is noted that the past three Presidents of the United States—William Clinton, George W. Bush, and Barack Obama—have all admitted to using illegal drugs at one or more times in their lives and still been elected and, in two cases, reelected.⁴⁹

These examples have sparked a new discussion regarding the power of the Internet. Since the online world is so vast and social networking sites like Myspace and Facebook and Internet content facilitators like DontDateHimGirl.com and

With Cannabis Pipe,” *News of the World*, January 2, 2009; Kevin Eason, “Drugs Claim Could Spell Disaster for Michael Phelps,” *Times Online*, February 2, 2009; Nicholas Graham, “Michael Phelps Bong Picture: Olympic Champion Caught Smoking Marijuana,” *Huffington Post*, February 5, 2009; “Phelps: Photo With Marijuana Pipe Real,” *ESPN*, February 2, 2009.

⁴⁷ Joseph DeMaio, “Negative Reactions Toward Phelps Photo Unjustified,” *The Heights*, March 16, 2009, Sports.

⁴⁸ Hulu, “Really?!?: Michael Phelps,” <http://www.hulu.com/watch/56636/saturday-night-live-really-michael-phelps#x-4,cNews%20and%20Politics,2> (accessed April 30, 2009).

⁴⁹ “Online Presence Will Balance Future Playing Field,” *The Heights*, March 9, 2009, Editorial.

AutoAdmit.com have made it easy to submit questionable or embarrassing content, it is possible that this concept of public shame will cease to exist in the future. The idea is that everyone will eventually have some picture, unflattering comment, or controversial content available on the Internet, and the novelty of these discoveries will wear off as they become more commonplace.⁵⁰ Furthermore, just as the privacy issue caught on in the context of social networking sites, perhaps the idea that information, especially content written about other people, on the Internet should be checked for its validity before it is to be passed off as fact. Sean Coit, a writer for *The Philadelphia Inquirer*, instructs the public to “enjoy the blog, but trust the paper.”⁵¹ His comment reflects a mature attitude and astute sense of cyber-literacy. Since the Internet is growing so quickly and gives every user an equal opportunity to post original content without being edited, monitored, or censored for the most part, Internet users must learn to doubt most of the content they read over the Internet. Unlike newspapers, which go through extensive fact-checking and editorial processes, the Internet simply does not have many filters in place to weed out lies or half-truths. As more and more visitors begin to come to this mature understanding of the nature of the Internet, defamatory statements will carry less and less weight coming from this source and even employers and universities may come to realize that they can not rely on this information. Taken as a whole, these developing social changes seem to imply that rather than changing Section 230, perhaps

⁵⁰ “Online Presence Will Balance Future Playing Field,” *The Heights*, March 9, 2009, Editorial.

⁵¹ Sean Coit, “Enjoy the Blog but Trust the Paper,” *The Philadelphia Enquirer*, April 27, 2009.

society and the Internet community have taken the first step in adapting themselves to an immunity-based World Wide Web.

Self-Regulation Standards as a Compromise

When Juicy Campus was still in existence, it was not just the website's request for "juice" that upset college students across the nation.⁵² While the website's pension for gossip was at times uncomfortable, undesirable, and unsavory to users, the issues with Juicy Campus also stemmed from the site's various features or, in some cases, lack thereof. Anonymity was the first big problem, as many students seemed to take Matt Investor's "100% Anonymous" promise to heart.⁵³ When it was uncovered that the site's anonymity was not impenetrable, a student who threatened violence at his university forced Juicy Campus site operators to divulge the student's IP address to the proper authorities, a collective sigh of relief was heard around the nation as it seemed that at

⁵² Juicy Campus, "Home," <http://juicycampus.com> (accessed January 23, 2009); Justin Pope, "'Juicy Campus' Website Could Hurt Students' Job Search," *WSLS 10*, February 18, 2008; The Legal Satyricon, "Gators Attack Juicy Campus," <http://randazza.wordpress.com/2008/07/31/gators-attack-juicy-campus/> (accessed April 29, 2009).

⁵³ Juicy Campus.

least some legal action could be possible when necessary.⁵⁴ Yet this information alone could not end the Juicy Campus debate.

Some feared that Juicy Campus's content would appear when employers conducted a Google search of the individual's name, leading them to the offending posts. Others expressed their unhappiness at the site's commenting format. Juicy Campus allowed users to post their thoughts regarding each individual post below it in a comments section, but some users complained about the fact that they could only comment once on a particular post. If someone were to come along and respond to their comment below it, their role in the conversation was already over leaving them unable to address certain claims or situations further. Still others were frustrated and frightened at the prospect of these posts remaining on Juicy Campus's Internet server forever, with no discernable expiration or deletion date in sight. Once something was posted to Juicy Campus, it seemed, it was there for good.⁵⁵

These concerns are legitimate, and it seems that Juicy Campus could have adjusted the infrastructure of their website to comply with these user requests. It is possible that Juicy Campus could have enjoyed the privileges of its immunity and maintained a hands off approach to policing or overseeing its content but still find a way

⁵⁴ Juicy Campus, "Privacy & Tracking Policy," <http://juicycampus.com/posts/privacy-policy> (accessed January 23, 2009).

⁵⁵ Summary derived from Caleb Daniloff, "Cyberbullying Goes to College: Online Harassment Can Turn Campus Life into a Virtual Hell," *BU Today*, April 22, 2009, Campus Life; Genna Tan, "Students Stand Up to Juicy Campus Website: Anonymous Online Blogging Affects Students' Self Esteem," *The Santa Clara*, November 6, 2008.

to add certain features which would have enhanced the interests and safety of its visitors. Taking into account all of the interests which need to be addressed and maintained if Section 230 is to be amended in any way, there are a few, less restrictive and burdensome means by which the area of online law could be improved. These methods are known as self-regulation tools which mostly allow users to address their grievances amongst themselves, with minimal involvement from the site operators and the courts. So long as the website operator sets up the tools necessary for this self-regulating format at the website's inception, the Internet is transformed into a much more user-friendly world. There are certain measures or site features which an ICF should add to their website—such as the right to reply, expiration dates, and flagging mechanisms—that would balance their own immunity with the issues plaguing their users. While government involvement should be minimal, there are certain policy ideas which Congress could enact to assist websites and users in their search for a compromise. Requiring websites to develop a formula for blocking search engines from compiling the content available on their servers and ensuring that these sites verify that visitors are using a valid IP address that is not being cloaked by a special program could serve as valuable additions to the existing legislation in this area.

Features Internet Content Facilitators Should Develop

While these social changes are developing, there are also certain measures that owners of Internet content facilitators could adopt to aid the development of the Internet and address some of the issues Juicy Campus failed to correct. While these features

should not necessarily be legally mandatory, they are to the benefit of an enhanced experience for users on the Internet, and site operators should view these new elements as a way to increase the flow of communication and organization of their websites. By addressing some of the original Juicy Campus user complaints, remaining and newly developing Internet content facilitators could increase customer approval ratings and augment their business.

The first of these suggestions is the right to reply. While Juicy Campus did allow for user comments, the website limited each visitor to one comment per topic. If another user's comment was a direct response to that user's comment, the original commenter was unable to contribute anything more to the conversation. Moreover, there are still several websites which do not allow for any kind of reply or additional commenting at all. As Justice Oliver Wendell Holmes, Jr., wrote in the dissenting opinion in *Abrams v. United States* (1919),

But when men have realized that time has upset many fighting faiths, they may come to believe even more than they believe the very foundations of their own conduct that the ultimate good desired is better reached by free trade in ideas...that the best test of truth is the power of the thought to get itself accepted in the competition of the market, and that truth is the only ground upon which their wishes safely can be carried out. That at any rate is the theory of our Constitution.⁵⁶

This quote sparked the rationale for freedom of expression known as the “marketplace of ideas,” a theory which holds that the truth or the best policy becomes apparent only

⁵⁶ *Abrams v. United States*, 250 U.S. 616 (1919).

through the competition of widely different ideas or sides in an argument in free-flowing public discourse. In order for the truth to prevail or the best idea to come forth, everyone must be given the opportunity to join the conversation. The best way to handle so-called “bad speech,” Holmes implies, is with more speech.⁵⁷

Keeping this theory in mind, it seems that the Internet would be enhanced if users were consistently given the right to reply to the postings of other users, especially when the content in question relates to them personally. This would allow viewers of the message to see both sides of the story instantaneously, and provides readers with a more informed decision as to the validity of the statement. Perhaps some users would even feel that their frustrations with the original message have been satisfied after posting a reply, and if so, this would help alleviate the amount of defamation suits being brought before the courts. While it would not eliminate the issue of online defamation completely, certainly there are some issues which could be remedied by providing a forum for better back-and-forth discussion and feedback.

The second issue relates to the length of time that these postings remain on the Internet. When Juicy Campus was at the height of its popularity, a common suggestion was that the site’s content should be assigned an expiration date. That way, students who felt they had been victimized could at least find comfort in knowing that this information could only be referred back to for so long. It should also be noted that aside from reasons directly related to defamation, Juicy Campus’s website became so cluttered with postings at one point that it was difficult to navigate. An argument could be made in favor of expiration dates on content simply on the basis of website aesthetics and operation

⁵⁷ 250 U.S. 616 (1919).

standards. If website operators chose not to maintain all of their content forever, it would ease some of the burden involved in facilitating such a site and make the website easier and more pleasant for users to navigate.

It was previously mentioned that re-posting is an issue on the Internet, especially with regards to copyright infringement. While a valid argument can be made against expiration dates for this very reason—once a post “expires” the original author or another user could simply re-post it to the website—this would probably only occur in instances where the original poster was extremely passionate about publishing this information. This user could be an individual with a valid or important message to disseminate, such as someone trying to alert the college campus that a professor is sexually harassing his students or that one of his peers has violent tendencies and is planning an attack on the campus. Conversely, this poster could simply be someone determined upon ruining the reputation of another individual and therefore re-posts the content so that others can continue to view it and add to the embarrassment. Such a situation may be the type of egregious offense that should be brought before the courts and dealt with in a legal manner.

Other than these two extreme viewpoints, it is likely that the majority of users will not mind that their content is expiring, because the very nature of these “gossip” sites is to have fresh or current information. The fact that “Timmy came out of the closet” or “Alicia flashed an entire fraternity” could be yesterday’s news, and the fact that these stories disappear and new ones replace them could accurately reflect the newsworthiness or relevance of third-party submitted content. Once the postings have been deleted after a certain period of time and site contributors move on to a different topic, the original

victim can find solace in the fact that information about them is no longer available to the public for viewing.

The final mechanism which Internet content facilitators should adopt involves a potential flagging or ratings system. On Amazon.com, users are allowed to write reviews for every product and service which is sold on the website. Additionally, though, users are allowed to rate other user reviews by voting on whether they found the review helpful or not. The “Was this review helpful to you?” feature alerts users and allows them to pick out quality reviews versus evaluations which may be less appealing.⁵⁸ Rating a review poorly will not eliminate it from the website, but this feature simply serves almost as a community standard available for assessment.

It is possible that a similar feature could benefit the community of users on Internet content facilitators. By flagging or rating posts, users can alert other visitors as to the quality or validity of the statement. Users can apply this information to read through the content more easily and utilize it as additional evidence should they ever doubt what they are viewing. Just like the Amazon website, this rating would not require operators to take any additional action, but if the website was in the practice of policing or reviewing their content, it could serve as an additional and valuable tool. By allowing the users to review the material and vote on its approval, website owners could alleviate themselves of the burden of having to sift through all of this information. If they chose to

⁵⁸ Amazon, “Was This Review Helpful to You?” http://www.amazon.com/Was-this-review-helpful-you/forum/Fx1JS1YLZ490S1O/Tx3QHE2JPEXQ1V7/1?_encoding=UTF8&asin=B000FL7CAU (accessed April 30, 2009).

do so, they could simply review the posts with very low approval ratings or a high number of flags and choose whether or not to delete or keep the content.

All three of these site features provide valuable new advantages for website operators and users alike. The right to reply allows for greater discourse and exchange of ideas on the Internet that could alleviate the amount of conversation taking place in the nation's legal system. Expiration dates not only eliminate potentially offensive content and prevent such statements from being available forever, but they also clean up a website's appearance and give way to more current information. Flagging and other rating systems are already in place at websites like Amazon.com, and not only do they serve as an evaluation of a community's standards, but they aid websites in locating unwanted or unacceptable content. Making these instruments industry standards could greatly benefit the overall Internet experience, especially for potentially defamed individuals.

Policy Ideas

While the government's involvement in this area should be kept to a minimum, there are two proposals that Congress should consider adopting. Internet content facilitators differ from Internet service providers and Internet content providers who either merely provide access to the Internet or content that comes from legitimate third-party news sources. If these ICFs are going to continue to facilitate, encourage, and collect what is often private or malicious information and take the privilege of Section 230 immunity beyond that of its predecessors, then perhaps Congress should require

Internet content facilitators to block the content of their sites from showing up in search engine results. Juicy Campus employed such a strategy during its life on the Internet, and explained to its users that if their name was entered into Google or any other search engine, Juicy Campus posts would not show up in the results.⁵⁹ While this may seem like a complicated technical process, a quick search of the Internet reveals that it is not. One website claims that blocking search engines from a website is “very simple” and explains how to do so.

You created your very own personal home on the web. However, the site turning up into search engines and web directories, revealing your personal details. It is very simple to block search engines from indexing your website by adding a small META code in your web pages and adding a small text file called robots.txt.

Protect your privacy.

Method 1

Add meta tag to head of your

```
<META NAME="ROBOTS" CONTENT="NOINDEX, NOFOLLOW">
```

Method 2

Create a robots.txt (all lower-case) using any simple text editor like Notepad.

Save it into your root directory of your domain to prevent search bots from

⁵⁹ Juicy Campus, “Frequently Asked Questions (FAQs),”

<http://juicycampus.com/faqs.php> (accessed July 15, 2008).

accessing any page on your site. Type the details exactly as give below into the robots.txt file

To exclude all robots from the entire server

User-agent: * Disallow: /

To allow all robots complete access

User-agent: * Disallow:

Or create an empty “/robots.txt” file.

To exclude all robots from part of the server

User-agent: * Disallow: /cgi-bin/ Disallow: /tmp/ Disallow: /private/

To exclude a single robot

User-agent: BadBot Disallow: /

To allow a single robot

User-agent: WebCrawler Disallow: User-agent: * Disallow: /⁶⁰

Two steps is all that is required of a probably experienced or knowledgeable online programmer or web designer to keep this content from being more easily accessible than necessary. If an Internet user wants to find the material in question, they can easily visit the website and search for it there.

⁶⁰ Online Quick Tips, “Block Search Engines from Indexing Site,”

<http://www.quickonlinetips.com/archives/2005/01/ways-to-prevent-search-engines-from-indexing-your-private-site/> (accessed April 30, 2009).

Such a policy would eliminate the fear of employers discovering information like Juicy Campus posts when they conduct an initial search of their potential hires on the Internet. It would also create a tighter sense of community amongst the users of a particular website. The fact that whatever activity takes place on the website stays within the confines of the site could instill a greater sense of trust between users and site operators. In addition, if search engines no longer have access to this information and Internet users are forced to visit the original site initially to obtain it, then that could potentially increase direct site traffic—a benefit website owners could surely rally behind.

Congress should also mandate that all Internet content facilitators require some form of IP address verification. What makes these websites so controversial in addition to all of the issues previously discussed is the anonymity they often provide users. Section 230 with no anonymity would not be an issue, because users would be able to identify the original poster and sue that individual for defamation. Section 230 combined with anonymity presents a bigger problem. With no way to identify the original author, the immunity that Section 230 provides websites leaves these victims angry and with no legal recourse. Keeping this dilemma in mind, Congress should require that these websites maintain IP addresses for all users. The IP address that users need in order to access the Internet is the most minimally intrusive form of record keeping that a website can maintain, and with it the possibility exists that the address can be traced back to the user if legal action needs to be taken.

Maintaining IP address records does not mean, however, that websites will automatically give up this information and violate the right to anonymity on the Internet

automatically. Victims would still have to go through the same legal process as before and obtain a court order to reveal this information. This is illustrated in the case *Dendrite International, Inc. v. John Doe No. 3* which involved a company, Dendrite, attempting to uncover the identity of certain anonymous posters who revealed company secrets and were violated insider trading policies on Yahoo! Bulletin boards.⁶¹ When one of these anonymous posters contested Dendrite's ability to uncover his identity, the court stated that

The complaint and all information provided to the court should be carefully reviewed to determine whether plaintiff has set forth a prima facie cause of action against the fictitiously-named anonymous defendants. In addition to establishing that its action can withstand a motion to dismiss for failure to state a claim upon which relief can be granted pursuant to R. 4:6-2(f), the 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.⁶²

Since Dendrite had not proved that they would be likely to win a defamation lawsuit against this individual on the merits of their argument as explained to the court, the judges denied the company the right to learn his true identity. This case demonstrates that although this information is available, the courts do not take the matter of unveiling a user's identity lightly and anonymity is still a valued aspect of the Internet. Whereas before there was a chance that attempting to uncover the IP address in hopes of

⁶¹ *Dendrite International, Inc. v. John Doe No. 3*, 342 N.J. Super. 134.

⁶² 342 N.J. Super. 134.

identifying the user would lead to faulty or nonexistent information, this verification system would guarantee that such a remedy was available if a court felt there was a legitimate cause of action.

Since some users do seek the help of IP-cloaking websites to conceal their identity from websites, Internet content facilitators should build in a verification system which does not grant a user access to their site unless an IP address can be identified and recorded. Once again, this type of system could be created by adding a section of computer programming code to the website's infrastructure. The steps for using the JavaScript programming version of this code are as follows:

<!-- TWO STEPS TO INSTALL VALIDATION (IP ADDRESS):

1. Copy the coding into the HEAD of your HTML document
2. Add the last code into the BODY of your HTML document -->

<!-- STEP ONE: Paste this code into the HEAD of your HTML document -->

[...]

<!-- STEP TWO: Copy this code into the BODY of your HTML document -->

[...] ⁶³

Two steps, both involving the copying of previously existing and available code, achieve the desired interface necessary to maintain this type of record keeping.

Both of these requests are not overly burdensome or intrusive as shown by the availability of the information necessary for their implementation already on the web. Nonetheless, they are important additions to Internet content facilitator's working

⁶³ Internet.com, "Validation (IP Address)," <http://javascript.Internet.com/forms/validation.html> (accessed April 30, 2009).

structure because they add some much needed assistance in the way of user privacy and protection. Due to their significance, perhaps Congress should step in and assist in these matters alone in order to further the interests of online defamation victims.

Conclusion

When the Internet first emerged as a truly powerful mass communication tool, it was lauded for its ability to provide every citizen with a forum for free expression. In keeping with this tradition, Section 230 of the Communications Decency Act was enacted to promote freedom of speech and the continued growth of the web. Unfortunately, this amount of liberty on the Internet has also led to the abuse of this privilege in the form of defamatory content. Moreover, the creation of websites like Juicy Campus which serve as Internet content facilitators has encouraged users to violate defamation and privacy laws. The initial reaction in situations where the law seems to be unbalanced is often to call for stricter governmental controls or increased legislation in the area of legal defense. In the case of Section 230 immunity, this is not the most advantageous solution.

Adjusting Section 230 to better serve the needs of defamation victims in a legal sense carries good intentions, but such reforms would bury the court system in a seemingly endless number of suits. It is neither to the benefit of the Internet content facilitator nor the victim to engage in a suing match to uncover the identity of the original poster or recover monetary damages. Social changes in attitude and behavior and self-regulatory tools provide the most sufficient compromise in this matter. As cyber-literacy increases and better infrastructures become the industry standard on the Internet, website

operators can continue to run their businesses without fear of losing immunity and their users can post and browse content knowing that their personal interests have been considered. Government interference is not the ultimate answer to the Section 230 problem, and the changes needed to clean up the Internet must begin with the people who use it.