

## The Big Bad Internet: Reassessing Service Provider Immunity Under § 230 to Protect the Private Individual from Unrestrained Internet Communication

Molly Sachson

Follow this and additional works at: <https://scholarship.law.stjohns.edu/jcred>

---

This Note is brought to you for free and open access by the Journals at St. John's Law Scholarship Repository. It has been accepted for inclusion in Journal of Civil Rights and Economic Development by an authorized editor of St. John's Law Scholarship Repository. For more information, please contact [selbyc@stjohns.edu](mailto:selbyc@stjohns.edu).

## THE BIG BAD INTERNET:

### REASSESSING SERVICE PROVIDER IMMUNITY UNDER § 230 TO PROTECT THE PRIVATE INDIVIDUAL FROM UNRESTRAINED INTERNET COMMUNICATION

MOLLY SACHSON

#### INTRODUCTION

For most Americans, surfing the Internet has become as much a part of their daily routine as getting dressed in the morning.<sup>1</sup> They can read the latest reports on the escalating oil prices or the approaching tropical storm,<sup>2</sup> send quick messages to friends and relatives about their son's first birthday,<sup>3</sup> check to see whether the Yankees beat the Red Sox,<sup>4</sup> or buy a pair of this season's most coveted Jimmy Choo stilettos.<sup>5</sup> They can also peruse or contribute to their favorite forums. Forums, which are special-interest group discussions, embody the "Internet at its liveliest."<sup>6</sup> There are thousands of forums on the Internet, dedicated to everything from cooking<sup>7</sup>

<sup>1</sup> According to a 2008 survey, over 74% of the American population used the Internet. Internet World Stats: Usage and Population Statistics, <http://www.internetworldstats.com/stats.htm> (last visited Nov. 18, 2009). This figure represents a 134% increase since 2000. *See id.*

<sup>2</sup> *See, e.g.*, CNN, <http://www.cnn.com> (last visited Nov. 18, 2009); National and Local Weather Forecast, Hurricane, Radar and Report, <http://www.weather.com> (last visited Nov. 18, 2009).

<sup>3</sup> *See, e.g.*, Gmail: Email from Google, <http://www.mail.google.com> (last visited Nov. 18, 2009); Meebo: Instant Messaging Everywhere, <http://www.meebo.com> (last visited Nov. 18, 2009).

<sup>4</sup> *See, e.g.*, ESPN: The World Leader in Sports, <http://www.espn.go.com> (last visited Nov. 18, 2009); CBS Sports, <http://www.sportsline.com> (last visited Nov. 18, 2009).

<sup>5</sup> *See, e.g.*, Bluefly: The Ultimate Hook-up for the Fashion Obsessed, <http://www.bluefly.com> (last visited Nov. 18, 2009).

<sup>6</sup> Journey to Forever: Internet Interaction, [http://journeytoforever.org/internet\\_how.html](http://journeytoforever.org/internet_how.html) (last visited Nov. 18, 2009). Forums are places where millions of people meet every day to "find like-minded friends, swap ideas and share resources." *Id.*

<sup>7</sup> *See* Discuss Cooking Forum and Community, <http://www.discusscooking.com> (last visited Nov. 18, 2009).

to salamanders.<sup>8</sup> Because Internet users from all over the world can access and contribute to these “self-help communities and clubhouses,”<sup>9</sup> forums have the potential to offer a wealth of invaluable information.<sup>10</sup> At the same time, however, forums may also foster harmful or illegal commentary.<sup>11</sup> As Internet forums and discussion boards continue to multiply, the private individual may become increasingly vulnerable to defamation, invasion of privacy, and infringement of constitutional rights.<sup>12</sup> Thus, the question arises: how do we protect the population from unbridled third-party forum postings?

An individual hoping to recover from a statement made in Cyberspace will run into two very serious obstacles. First, he will most likely be unable to identify the third-party responsible for the commentary since most forum postings are made anonymously.<sup>13</sup> Internet service providers who feature chat rooms and forums on their websites afford users this anonymity through the mechanism of “user names,”<sup>14</sup> which allow people

<sup>8</sup> See Caudata.org: The Newt and Salamander Portal, <http://www.caudata.org/index.php> (last visited Nov. 18, 2009).

<sup>9</sup> Journey to Forever: Internet Interaction, [http://journeytoforever.org/internet\\_how.html](http://journeytoforever.org/internet_how.html) (last visited Nov. 18, 2009).

<sup>10</sup> See *id.* (noting that discussions in forums “accumulate into databases that are a mine of useful information”); see also *ACLU v. Reno*, 929 F. Supp. 824, 844 (E.D. Pa. 1996) (explaining that the Internet is a “unique and wholly new medium of worldwide human communication”).

<sup>11</sup> See, e.g., *Doe I v. Individuals*, 561 F. Supp. 2d 249, 251 (D. Conn. 2008) (noting that a discussion board linked a photograph of a young woman and displayed messages describing the alleged criminal history of the woman’s father, accusing the woman of abusing heroin, fantasizing about being raped by her father, and having a sexually transmitted disease); *Chicago Lawyers’ Comm. for Civil Rights Under Law, Inc. v. Craigslist, Inc.*, 519 F. 3d 666, 668 (7th Cir. 2008) (discussing a forum for individuals looking to buy, sell, or rent housing that included postings claiming “no minorities” and “no children” in violation of the Fair Housing Act); *Carafano v. Metrosplash.com, Inc.*, 339 F.3d 1119, 1121 (9th Cir. 2003) (examining a dating website which displayed a fabricated profile indicating that a well-known actress was “looking for a one-night stand” and a man with a “strong sexual appetite”).

<sup>12</sup> See DANIEL J. SOLOVE, *THE FUTURE OF REPUTATION: GOSSIP, RUMOR, AND PRIVACY ON THE INTERNET* 4 (Yale University Press 2007) (suggesting that there is a “dark side” to the Internet that poses threats to “people’s control over their reputations and their ability to be who they want to be”); see also Lilian Edwards, *Defamation and the Internet: Name Calling in Cyberspace*, in *LAW AND THE INTERNET: REGULATING CYBERSPACE* (1997), available at [http://www.law.ed.ac.uk/it&law/c10\\_main.htm](http://www.law.ed.ac.uk/it&law/c10_main.htm) (describing how discussion fora are a part of the “defamation prone zone” of the Internet).

<sup>13</sup> See Christopher Butler, *Plotting the Return of an Ancient Tort to Cyberspace: Towards a New Federal Standard of Responsibility for Defamation for Internet Service Providers*, 6 MICH. TELECOMM. & TECH. L. REV. 247, 260 (2000) (indicating that one of the “great[est] stumbling block[s]” that a person who has been defamed or injured in Cyberspace might face is the “ease with which the medium facilitates anonymity”) (alterations in original); ROBERT A. GORMAN & JANE C. GINSBURG, *COPYRIGHT* 899 (7th ed. 2006) (explaining that while it may be possible to discover the Internet provider address of an online third-party, it will be very difficult to ascertain the actual name of the person corresponding to that provider address).

<sup>14</sup> See, e.g., *Doe I*, 561 F. Supp. 2d at 250–51 (discussing that an individual posted the explicit remarks about the plaintiff under the pseudonym “AK47”); see also SOLOVE, *supra* note 12, at 139 (noting that 55 percent of bloggers use pseudonyms instead of their real names (citing Amanda Lenhart & Susannah Fox, *Bloggers: A Portrait of the Internet’s New Storytellers*, PEW INTERNET & AMERICAN LIFE PROJECT, July, 19, 2006, <http://www.pewinternet.org/pdfs/PIP%20Bloggers%20Report%20July%20>

to post anything without facing criticism for their views or repercussions for their insults.<sup>15</sup> Second, if he sues the website provider in lieu of the unidentified poster, he will have to contend with § 230 of the Communications Decency Act (“§ 230”).<sup>16</sup> This provision creates immunity for an interactive computer “service provider” in any cause of action that would make him liable for information originating with “another information content provider.”<sup>17</sup> Therefore, unless the website provider was also acting as another “content provider,” the plaintiff’s claim will likely be dismissed.

Determining whether a website provider, or “webhost,” has acted as a “content provider,” however, may not always be an easy task. When a website provider creates an Internet discussion board dedicated to a topic such as celebrity gossip,<sup>18</sup> but does not contribute to the ongoing discourse or supervise the activities of its users,<sup>19</sup> it is fairly clear that he is simply a service provider. In contrast, if in addition to providing a forum for third parties to discuss the celebrity gossip, the webhost also broadcasts his own personal opinions and general commentary on the subject matter,<sup>20</sup> he is a content provider.

With that in mind, how would the courts characterize a website provider who does not necessarily express his own viewpoint, but who guides the subject matter of the subscribers’ postings by posing provocative questions?<sup>21</sup> For example, consider a celebrity gossip forum in which the webhost asks his subscribers: “What do you think of Tom Cruise? Did anyone see his latest movie that tanked in the box office?” The website provider does not express his personal opinions about or criticisms of Tom

2019%202006.pdf)).

<sup>15</sup> See Butler, *supra* note 13, at 260–61 (suggesting that “[a]nonymity has been both one of the most praised and vilified features of the Internet” because on one hand, it allows people to post their opinions without the fear of harassment and on the other hand, it allows people to seriously damage another individual’s reputation without the fear of getting caught); Anthony Ciolli, *Chilling Effects: The Communications Decency Act and the Online Marketplace of Ideas*, 63 U. MIAMI L. REV. 137, 137, 156–57, 2008 (discussing how the Internet has made speech completely free, but presents obstacles in defamation claims where the speech is anonymous).

<sup>16</sup> 47 U.S.C. § 230 (1996).

<sup>17</sup> *Id.* at § 230(c).

<sup>18</sup> See, e.g., About.com, *Celebrity Gossip*, <http://forums.about.com/n/pfx/forum.aspx?nav=messag&webtag=ab-gossip> (last visited Oct. 6, 2008); see also IVillage Celebrity Chatter, <http://messageboards.ivillage.com/iv-enmovies> (last visited Nov. 15, 2009).

<sup>19</sup> See About.com, *supra* note 18; IVillage Celebrity Chatter, *supra* note 18.

<sup>20</sup> See, e.g., Celebrity Gossip Blog from Perez Hilton, <http://www.perezhilton.com> (last visited Sept. 28, 2008) (broadcasting webhost’s personal opinions and creating a forum for third parties’ commentary); Gossip Center, <http://www.celebrity-gossip.net/> (last visited Nov. 15, 2009) (creating celebrity gossip headlines and opportunities for third parties to comment).

<sup>21</sup> See, e.g., Celebrity Gossip Blog from Perez Hilton, <http://www.perezhilton.com> (last visited Nov. 15, 2008) (posing provocative questions to website subscribers).

Cruise, but he does induce his subscribers to do so. By encouraging responses from third parties, the webhost is arguably doing more than providing the service – he is indirectly creating content because without his question, the harmful response might never have been made. Be that as it may, he is not necessarily a content provider because he is not directly creating the information himself. Thus, his actions fall somewhere within the gray area between “content provider” and “service provider.”

Because the methods available to a website provider do not always fit neatly into categories of content providing or service providing, it seems unwise to base the decision of immunity solely on this dichotomy. If the courts continue to rely on this, website providers who have in fact been responsible for the dissemination of tortious or illegal language, perhaps because they have solicited the comments from third parties through provocative questions, may escape liability if the court happens to determine that they were simply “service providers.” Thus, the individual may be deprived of a recovery. In order to prevent such unfair results, the courts must reassess the extent of protection provided under § 230 and consider extending liability to webhosts in certain situations, perhaps even where they are solely acting as service providers.

This Note examines the precise terms of § 230 and suggests that the statute should not be interpreted broadly as granting absolute blanket immunity to all Internet service providers. Rather, this Note argues that a more narrow interpretation of § 230 that imposes liability under limited circumstances is consistent with Congressional intent and the authority of First Amendment law. Such an interpretation will also have the beneficial effect of encouraging website providers to act more responsibly in screening for illegal or tortious content, thereby protecting the private individual’s right to be free from discrimination, defamation, and invasion of privacy.

Part I provides a brief summary of the original approach to Internet service provider liability and examines the policy rationales behind the enactment of § 230. Part IIA illustrates the widespread judicial preference for interpreting § 230 as providing broad, robust immunity for Internet service providers. Part IIB, however, highlights a recent opinion from the Ninth Circuit that diverged from the trend of granting absolute immunity and held a website provider liable for developing discriminatory content in violation of the Fair Housing Act. Part III evaluates the arguments on both sides of the debate over the extent of webhost immunity in order to underscore the importance of the issues at stake in the circuit split.

Part IV suggests that the Ninth Circuit’s decision to limit the broad scope

of immunity under § 230 was a necessary step in the right direction. Extending liability will protect the private person's ability to be free from illegal or tortious third-party attacks without undermining Congress's intent to promote the growth of the Internet. This Note proposes that the standard for imposing liability should not depend solely on whether the webhost was a service provider or a content provider. Rather, the standard should focus on the extent to which the nature of the website was such that it should have put the Internet service provider on notice of the risk of illegal or tortious postings.

### I. THE ROAD TO § 230

The extent of liability for Internet providers has been in flux since the earliest days of the Internet. In the early 1990's, the courts granted immunity in situations where it was apparent that the website provider was acting as a distributor, as opposed to a publisher, of information.<sup>22</sup> To make this distinction, the courts focused on the degree of editorial control that the provider exercised over the content on his website.<sup>23</sup> If the webhost did not review anything before displaying it on the forum, the courts often treated him as the "functional equivalent of a more traditional news vendor."<sup>24</sup> Thus, the courts would not likely impute knowledge of the disputed material to him.<sup>25</sup> In contrast, if the webhost monitored, edited, or removed content from his website,<sup>26</sup> the courts treated him as a publisher of information.<sup>27</sup> As such, he would be liable for unlawful commentary if he failed to delete or alter it.<sup>28</sup>

One problem with this approach was that the analogy between an Internet service provider and a traditional news distributor, such as a

<sup>22</sup> *Cubby, Inc. v. CompuServe, Inc.*, 776 F. Supp. 135, 139–40 (S.D.N.Y. 1991) (granting immunity in situations where it was clear that the website provider was acting as a distributor rather than a publisher of information).

<sup>23</sup> See *id.* at 140 (noting that the webhost had no more editorial control over publication "than does a public library, book store, or newsstand").

<sup>24</sup> *Id.*

<sup>25</sup> See *id.* at 141 (agreeing that the webhost acted as a distributor and thus had neither knowledge nor reason to know of the allegedly defamatory statements on his website, especially given the large number of publications it carried and the speed with which the webhost uploaded third-party content and made it available to subscribers); see also Robert T. Langdon, Note, *The Communications Decency Act § 230: Make Sense? Or Nonsense? – A Private Person's Inability to Recover if Defamed in Cyberspace*, 73 ST. JOHN'S L. REV. 829, 841 (1999) (noting that distributors, such as bookstores or newsstands, are not expected to monitor the contents of every book or magazine they sell).

<sup>26</sup> See *Stratton Oakmont, Inc. v. Prodigy Servs. Co.*, 1995 N.Y. Misc. LEXIS 229 at \*10 (N.Y. Sup. Ct. May 24, 1995).

<sup>27</sup> *Id.* at \*10–11.

<sup>28</sup> *Id.* at \*11.

bookstore or newsstand, was flawed. First, a website provider plays a very different role in supplying information and ideas than does the traditional distributor. Specifically, the website provider typically has no knowledge of an author's identity or the subject matter of the postings, whereas a bookstore or newsstand is usually involved to some extent in the selection of merchandise.<sup>29</sup> Second, a website provider is distinguishable because he is not necessarily motivated by the need to maintain a reputation for accurate reporting. A traditional distributor must uphold such a reputation because if he starts to provide poor quality information, customers may be deterred from making purchases in the future. An Internet service provider, in contrast, will probably not suffer if he supplies inferior information because the public does not always expect perfect accuracy;<sup>30</sup> it expects a forum for diverse and compelling ideas.<sup>31</sup> Because website providers are not in effect comparable to news distributors, an approach that attempts to treat them the same is fundamentally unsound. A more serious problem with the original approach, however, was that it had the effect of discouraging good faith self-policing on the part of website providers who feared being treated as publishers.<sup>32</sup>

In 1996, Congress enacted § 230 in an effort to address the problems of the distributor-publisher approach and to mitigate its harsh consequences. Section 230(c), which is entitled "Protection for 'good Samaritan' blocking and screening of offensive material," grants immunity for any actions "voluntarily taken in good faith to restrict access to or availability of"

<sup>29</sup> See, e.g., Butler, *supra* note 13, at 258 (confirming that the website operator in *Stratton Oakmont* did not "solicit articles or pay the participants"); see also Jac Hong Lee, Batzel v. Smith & Barrett v. Rosenthal: *Defamation Liability for Third-party Content on the Internet*, 19 BERKELEY TECH. L. J. 496, 471 (2004) (discussing how booksellers merely distribute their content).

<sup>30</sup> See Butler, *supra* note 13, at 259. "Unlike the assertions made in a newspaper or magazine, which have an extra veneer of truth because the public knows the articles are approved and commissioned by editors, the public likely holds no similar illusions about the postings in a public forum." *Id.*; see also *Stratton Oakmont*, 1995 Misc. LEXIS at \*6 (noting the willingness to discuss the variety of information that can be posted).

<sup>31</sup> See Butler, *supra* note 13, at 259 (noting that the website operator in *Stratton Oakmont*, who was fully "committed to open debate and discussion," never made any assertion about the reliability of the postings on the website (quoting *Stratton Oakmont*, 1995 N.Y. Misc. LEXIS 229 at \*6)); see also Jay Krasovec, *Cyberspace: The Final Frontier, for Regulation?* 41 AKRON L. REV. 101, 102 (1997) (discussing the diversity of ideas on the internet).

<sup>32</sup> See *Fair Hous. Council v. Roomates.com, LLC*, 521 F.3d 1157, 1163 (9th Cir. 2008) (indicating that "under *Stratton Oakmont*, online service providers that voluntarily filter some messages become liable for all messages transmitted, whereas providers that ignore problematic posts altogether escape liability"); see also David R. Sheridan, *Zeran v. AOL and the Effect of § 230 of the Communications Decency Act upon Liability for Defamation on the Internet*, 61 ALB. L. REV. 147, 158 (1997) (emphasizing the fact that a website provider who assumes the responsibility for at least attempting to keep offensive content off his website will be liable for any illegal or tortious postings – but an operator who makes no such responsible attempt will escape all liability).

offensive material.<sup>33</sup> The act also provides that “no provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider.”<sup>34</sup> The language of § 230 plainly suggests that courts may not hold a website provider liable for performing traditional editorial functions.<sup>35</sup> Thus, § 230 effectively overrules past decisions where website providers were treated as publishers of content simply because they restricted access to other information on the website.<sup>36</sup>

Congress passed § 230 with two basic policy rationales in mind.<sup>37</sup> First, it hoped to promote the self-regulation of Internet service providers by removing the threat of potential liability for editing third-party content.<sup>38</sup> Second, it sought to “promote the continued development of the Internet” and encourage the free exchange of ideas.<sup>39</sup> In the statutory findings, Congress noted that the Internet, which has provided a “forum for a true diversity of political discourse, unique opportunities for cultural development, and myriad avenues for intellectual activity,”<sup>40</sup> has flourished

<sup>33</sup> 47 U.S.C. § 230(c)(2)(A) (1996).

<sup>34</sup> *Id.* at § 230(c)(1). An “information content provider” is “any person or entity that is responsible, in whole or in part, for the creation or development of information provided through the Internet or any other interactive computer service.” *Id.* § 230(f)(3). An “interactive computer service” is “any information service, system, or access software provider that provides or enables computer access by multiple users to a computer server[.]” *Id.* § 230(f)(2).

<sup>35</sup> See *Zeran v. America Online, Inc.*, 129 F.3d 327, 330 (4th Cir. 1997) (explaining that courts are precluded from entertaining claims that seek to hold a website provider liable for “its exercise of a publisher’s traditional editorial functions – such as deciding whether to publish, withdraw, postpone or alter content”); *Doe v. Friendfinder Network, Inc.*, 540 F. Supp. 2d 288, 298 (D.N.H. 2008) (noting that “a service provider’s exercise of its editorial prerogatives as to information from another content provider does not transform the service provider into the content provider under § 230”).

<sup>36</sup> See *Roommates.com*, 521 F.3d at 1163 (noting that the House Conference Report explicitly indicated that one purpose of § 230 was to “overrule *Stratton-Oakmont* [sic] v. *Prodigy* and any other similar decisions” (citing H.R. REP. NO. 104-458 (1996) (Conf. Rep.), as reprinted in 1996 U.S.C.C.A.N. 10)); see also Landgon, *supra* note 25, at 844 (explaining that § 230 overruled *Stratton-Oakmont* so that providers who filter out certain content will not be deemed to have exercised editorial control).

<sup>37</sup> See generally 47 U.S.C. § 230(b) (outlining the policies behind the Communications Decency Act); see also Eric M. D. Zion, *Protecting the E-Marketplace of Ideas by Protecting Employers: Immunity for Employers Under Section 230 of the Communications Decency Act*, 54 FED. COMM. L.J. 493, 505 (2002) (discussing the rationales behind section 230 of the Communications Decency Act).

<sup>38</sup> See § 230(b)(3) (“It is the policy of the United States ... (3) to encourage the development of technologies which maximize user control over what information is received by individuals, families, and schools who use the Internet and other interactive computer services[.]”); see also Chicago Lawyers’ Comm. for Civil Rights Under Law, Inc., v. Craigslist, Inc., 519 F.3d 666, 669–70 (7th Cir. 2008) (“Removing the risk of civil liability may induce web hosts and other informational intermediaries to take more care to protect the privacy and sensibilities of third parties.” (quoting *Doe v. GTE Corp.*, 347 F.3d 655 (7th Cir. 2003))).

<sup>39</sup> See 47 U.S.C. § 230(b)(1) (identifying the promotion of the continued development of the Internet as one of the policy reasons behind the Act); *Carafano v. Metrosplash.com, Inc.*, 339 F.3d 1119, 1122 (9th Cir. 2003) (stating that the promotion of the free exchange of ideas was one of the policy reasons for the act (citing *Batzel v. Smith*, 333 F.3d 1018, 1026–27 (9th Cir. 2003))).

<sup>40</sup> 47 U.S.C. § 230(a)(3).



to the benefit of the people largely without government intervention.<sup>41</sup> Thus, it was Congress's policy to "preserve the vibrant and competitive free market that exists for the Internet . . . unfettered by Federal or State regulation."<sup>42</sup>

## II. INTERPRETING THE EXTENT OF IMMUNITY UNDER § 230

### A. *The Traditional Understanding of § 230: Robust or Bust*

Historically, the courts have interpreted § 230 broadly.<sup>43</sup> Since its enactment, the courts have consistently adopted an "expansive definition of 'interactive computer service' and a relatively restrictive definition of 'information content provider.'"<sup>44</sup> They have justified their liberal understanding of the statute by arguing that extensive webhost immunity is consistent with the congressional policy concerns.<sup>45</sup>

The effect of the courts' expansive understanding of the statute has been that as long as the information has been provided by a third party, website operators will be absolutely immune from liability.<sup>46</sup> One of the earliest cases to apply § 230 was *Zeran v. America Online, Inc.*<sup>47</sup> There, an anonymous person posted a message on an America Online bulletin board advertising the sale of T-shirts with distasteful slogans about the Oklahoma City bombing.<sup>48</sup> The advertisement encouraged people who were interested

<sup>41</sup> See *id.* § 230(a)(4) ("The Internet and other interactive computer services have flourished, to the benefit of all Americans, with a minimum of government regulation.").

<sup>42</sup> See *id.* § 230(b)(2); see also *Zeran v. America Online, Inc.*, 129 F.3d 327, 330 (4th Cir. 1997) ("Section 230 was enacted, in part, to maintain the robust nature of Internet communication and, accordingly, to keep government interference in the medium to a minimum.").

<sup>43</sup> See *Carafano*, 339 F.3d at 1123 (characterizing immunity under § 230 as "quite robust"); see also Cecilia Ziniti, *The Optimal Liability System for Online Service Providers: How Zeran v. America Online Got it Right and Web 2.0 Proves It*, 23 BERKELEY TECH. L.J. 583, 585 (2008) (indicating that website providers have enjoyed immunity for a wide range of legal claims, including defamation, employment torts, breach of contract, and negligent misrepresentation).

<sup>44</sup> *Carafano*, 339 F.3d at 1123. See generally § 230(f)(2–3) (defining the terms "interactive computer service" and "information content provider").

<sup>45</sup> See *Carafano*, 339 F.3d at 1122–23 (noting that reviewing courts have been generous in granting immunity in light of Congress' goal to encourage the free exchange of ideas and the voluntary monitoring of offensive content); see also Ziniti, *supra* note 43, at 585 (suggesting that the courts' broad construction of § 230 most likely "stems from the statute's stated aims" in section 230(b)).

<sup>46</sup> See *Roomates.com*, 521 F.3d at 1180 (McKeown, C.J., dissenting) (indicating that website providers will be immune for basically anything that third parties post on a website, including "auctions of paintings that may have been stolen by Nazis [or] biting comments about steroids in baseball" (citing *Chicago Lawyers' Comm. for Civil Rights Under Law, Inc. v. Craigslist, Inc.*, 519 F.3d 666, 671 (7th Cir. 2008))); *Carafano*, 339 F.3d at 1123 (remarking that § 230(c) provides broad immunity for publishing content provided primarily by third parties).

<sup>47</sup> 129 F.3d 327 (4th Cir. 1997).

<sup>48</sup> *Id.* at 329.

in purchasing the T-shirts to call the plaintiff's home telephone number.<sup>49</sup> After receiving a deluge of calls from angry Internet users, the plaintiff requested that America Online remove the posting.<sup>50</sup> Although America Online complied, the anonymous party posted a similar posting the next day.<sup>51</sup> The Fourth Circuit held that America Online was immune from liability because it fell within the traditional definition of a publisher,<sup>52</sup> and by the explicit terms of § 230, the courts are prohibited from "entertaining claims that would place a computer service provider in a publisher's role."<sup>53</sup> The court further noted that even if America Online had acted as a distributor, it would not have been precluded from the protection of § 230.<sup>54</sup> The court indicated that in passing § 230, "Congress made a policy choice . . . not to deter harmful online speech through the separate route of imposing tort liability on companies that serve as intermediaries for their parties' potentially injurious messages."<sup>55</sup>

A few years after the decision in *Zeran*, the Ninth Circuit reiterated the wide scope of § 230 immunity in *Carafano v. Metrosplash.com*.<sup>56</sup> In that case, a dating website had allowed an unidentified party to post a personal profile for a popular actress without the actress's knowledge or consent.<sup>57</sup> As a result of the provocative posting, the actress began to receive a number of phone calls, messages, and e-mails from individuals who were interested in meeting her.<sup>58</sup> The actress's assistant eventually learned of the

<sup>49</sup> *Id.*

<sup>50</sup> *See id.* (explaining that most of the calls contained angry or derogatory messages, but some of the calls comprised of death threats).

<sup>51</sup> *See id.* The second posting, which also advertised the sale of T-shirts related to the bombing, further encouraged interested parties to call the plaintiff's number. *Id.* The post said: "please call back if busy" because there was such a large demand for the shirts. *Id.* As a result, the angry telephone calls escalated. *Id.* Over the next several days, the anonymous party continued to post advertisements for the sale of miscellaneous Oklahoma City bombing merchandise, including bumper stickers and key chains. *Id.*

<sup>52</sup> *See Zeran*, 129 F.3d at 332. Although the plaintiff sued America Online for negligence, the court found that his claim was "indistinguishable from a garden variety defamation action." *Id.* Thus, the court analyzed the case as if the plaintiff had sued for defamation. *Id.* Because those who "[take] part in publication [are] charged with publication" under defamation law, the court found that America Online was a publisher. *Id.* (quoting W. PAGE KEETON ET AL., PROSSER AND KEETON ON THE LAW OF TORTS § 113, at 799 (5th ed. 1984)).

<sup>53</sup> *Id.* at 330.

<sup>54</sup> *See id.* at 332 ("[Distributor] liability is merely a subset, or a species, of publisher liability, and is therefore also foreclosed by § 230.").

<sup>55</sup> *Id.* at 330–31.

<sup>56</sup> 339 F.3d 1119 (9th Cir. 2003) (finding an internet dating service immune from liability pursuant to § 230).

<sup>57</sup> *See id.* at 1121. The profile contained several pictures of the actress, as well as a description of her interests and appearance. *Id.* The profile indicated that the actress was "looking for a one night stand," and a "hard dominant" man with a "strong sexual appetite." *Id.* The profile also listed her address and home telephone number. *Id.*

<sup>58</sup> *See id.* At least one of the correspondences was sexually explicit and threatening. *See id.*

improper posting and contacted the dating website to demand that the profile be removed.<sup>59</sup> In spite of the “utterly deplorable consequences” of the wrongful posting, the court held that the dating website was protected from liability under § 230.<sup>60</sup> The court was persuaded that § 230 granted “robust” immunity<sup>61</sup> – especially for content provided primarily by third parties.<sup>62</sup> In fact, the court insisted that immunity applies even where the information is provided in response to a website’s detailed questionnaire.<sup>63</sup> The Ninth Circuit opined that unless the webhost “create[s] or develop[s] the particular information at issue,” the claim against him will be barred under § 230.<sup>64</sup>

In a more recent case, *Chicago Lawyers’ Committee for Civil Rights Under Law, Inc. v. Craigslist, Inc.*,<sup>65</sup> the Seventh Circuit joined the consensus that immunity under § 230 is “robust.” Craigslist is a forum for individuals who are interested in, among other things, buying, selling or renting housing.<sup>66</sup> Lawyers’ Committee claimed that the postings on the website proclaiming “no minorities” and “no children”<sup>67</sup> violated the Fair Housing Act.<sup>68</sup> The court, however, declined to extend liability to Craigslist because as a mere messenger of the illegal content, it was immune under § 230.<sup>69</sup> The court conceded that Craigslist played a causal role in the publication of the content to the extent that “no one could post a discriminatory ad if [it] did not offer a forum.”<sup>70</sup> Causation under the Fair Housing Act, however, refers to “causing . . . the discriminatory content of

<sup>59</sup> See *id.* at 1122. The website temporarily blocked the profile from public view, but then fully deleted the posting the next morning. *Id.*

<sup>60</sup> *Id.* at 1125.

<sup>61</sup> *Id.* at 1123 (indicating that broad immunity under § 230 has developed in light of the policy reasons underlying the statute). See *supra* note 45 and accompanying text.

<sup>62</sup> *Carafano*, 339 F.3d at 1124 (“Under § 230(c) . . . so long as a third party willingly provides the essential published content, the interactive service provider receives full immunity regardless of the specific editing or selection process.”).

<sup>63</sup> See *id.* at 1124–25. The plaintiff argued that the dating website contributed content to the website by asking detailed questions and providing a menu of “pre-prepared responses.” *Id.* The court, however, did not find that website was responsible for the underlying content. *Id.*

<sup>64</sup> *Id.* at 1125. The dating website did not create or develop the content at issue in this case because the critical information, such as the actress’s home address and phone number and the sexually suggesting comments, was transmitted to the website unaltered by the webhost. See *id.*

<sup>65</sup> 519 F.3d 666 (7th Cir. 2008).

<sup>66</sup> *Id.* at 668.

<sup>67</sup> *Id.*

<sup>68</sup> See 42 U.S.C. § 3604 (1988) (prohibiting certain forms of discrimination on the basis of “race, color, religion, sex, familial status, or national origin”).

<sup>69</sup> See *Craigslist*, 519 F.3d. at 672 (explaining that the plaintiff “cannot sue the messenger just because the message reveals a third party’s plan to engage in unlawful discrimination”).

<sup>70</sup> *Id.* at 671.

a statement.”<sup>71</sup> Because Craigslist did not encourage its subscribers in anyway to express their discriminatory preferences, the court held that it was simply a distributor and thus protected by § 230’s immunity.<sup>72</sup>

*B. The Ninth Circuit Limits the Scope of § 230 Immunity*

In the wake of the swelling support for broad immunity under § 230,<sup>73</sup> the Ninth Circuit made a decisive split from the other circuit courts in *Fair Housing Council of San Fernando Valley v. Roommates.com, LLC*.<sup>74</sup> Roommates.com is a website that purports to match people looking for housing with people who are renting out spare rooms.<sup>75</sup> In order to use the website’s services, the subscriber must create a profile describing himself with respect to three criteria provided in drop-down menus: sex, sexual orientation and whether he will bring children to the home.<sup>76</sup> After that, the subscriber must specify the type of roommate that he is looking for based on the same three criteria.<sup>77</sup> Roommates.com then publishes the subscriber’s responses, thereby making his information available to fellow subscribers looking for a roommate.<sup>78</sup>

Fair Housing Council contended that Roommates.com’s business violated the Fair Housing Act<sup>79</sup> and the state housing discrimination

<sup>71</sup> *Id.*

<sup>72</sup> See *id.* at 671–72 (noting further that Craigslist might have been deemed to have “caused” the discriminatory content if it had offered a lower price to people who included discriminatory statements in their postings).

<sup>73</sup> See, e.g., *Ben Ezra, Weinstein, and Co. v. America Online Inc.*, 206 F.3d 980 (10th Cir. 2000) (declining to extend liability to a website provider that displayed incorrect information about the plaintiff’s stock price and share volume on multiple occasions); *Doe v. Friendfinder Network, Inc.*, 540 F. Supp. 2d 288 (D.N.H. 2008) (holding an adult website immune under § 230 for false and unauthorized personal advertisements posted on its website by a third-party); *Noah v. AOL Time Warner Inc.*, 261 F. Supp. 2d 532, 535 (E.D. Va. 2003) (granting immunity under § 230 to an Internet service provider being sued for inadequately policing chat rooms where Muslims were “harassed, insulted, threatened, ridiculed and slandered” by other chat room participants).

<sup>74</sup> 521 F.3d 1157 (9th Cir. 2008).

<sup>75</sup> *Id.* at 1161.

<sup>76</sup> *Id.* Creating a profile is a strict condition of using Roommates.com; the subscriber cannot advertise housing opportunities or peruse any listings if he does not have a profile. *Id.*

<sup>77</sup> See *id.* The drop-down menus provide the subscriber the option to indicate whether he is willing to live with “straight or gay” males, only with “straight” males, only with “gay” males, or with “no males.” See *id.* at 1165. The subscriber must also choose either “I will live with children” or “I will not live with children” from the drop-down menus. See *id.* The subscribers have an opportunity to elaborate on their preferences in the “Additional Comments” section. *Id.* at 1161.

<sup>78</sup> See *id.* at 1165. The responses are included in the profile page to help other subscribers efficiently sort through the large number of people looking for a roommate. *Id.* If a subscriber is only looking for a gay male roommate, he will be able to easily find which subscribers do not fit that description by looking at the profile. See *id.*

<sup>79</sup> See 42 U.S.C. § 3604 (2006) (prohibiting discrimination in the sale or rental of housing on the basis of race, color, religion, sex, familial status, or national origin).

laws.<sup>80</sup> Fair Housing Council's claim was two-fold. First, it claimed that in requiring individuals to answer the profile questions as a precondition to using the website, Roommates.com unlawfully forced its subscribers to make discriminatory statements<sup>81</sup> concerning the sale or rental of housing in violation of § 3604.<sup>82</sup> Second, Fair Housing Council suggested that the website's "development and display" of the subscribers' discriminatory preferences was in itself unlawful.<sup>83</sup>

Notwithstanding a vigorous dissent,<sup>84</sup> the Ninth Circuit agreed with Fair Housing Council and held that Roommates.com was not protected by § 230 immunity. The thrust of the court's argument was that Roommates.com was acting as an "information content provider," and thus fell outside the scope of § 230.<sup>85</sup> An "information content provider," as defined in § 230, is "any person or entity that is responsible, in whole or in part, for the creation or development of information provided through the Internet[.]"<sup>86</sup> The court explained that in requiring its subscribers to provide answers based on a set of pre-selected, discriminatory choices as a condition to using the website's service,<sup>87</sup> Roommates.com effectively "developed" the

<sup>80</sup> See CAL. GOV'T CODE § 12955 (2009) (prohibiting the owner of any housing accommodation from discriminating on the basis of "race, color, religion, sex, sexual orientation, marital status, national origin, ancestry, familial status, source of income, or disability").

<sup>81</sup> A subscriber's answers to the profile questions are discriminatory because they indicate a preference to only live with certain kinds of people. If a subscriber claims, using the drop-down menu, that he is only interested in living with straight males without children, this implies that he is not willing to live with females, gay individuals or individuals with children. The menu lacks a "no preference" option and therefore the subscriber's answers will necessarily be discriminatory against some groups of people. Furthermore, the subscriber's responses to the profile questions may also cause other subscribers to discriminate against him. If he is a straight male, and another subscriber is seeking a gay male roommate, that other subscriber will not consider him as a possible roommate. Such discrimination on the basis of sexual orientation is a violation of the Fair Housing Act.

<sup>82</sup> See *Roommates.com*, 521 F.3d at 1165. Councils interpret the precondition that subscribers answer questions before being able to use the website as "unlawfully 'caus[ing]' subscribers to make a 'statement . . . with respect to the sale or rental of a dwelling that indicates [a] preference, limitation, or discrimination,' in violation of 42 U.S.C. § 3604(c)." *Id.*

<sup>83</sup> *Id.*

<sup>84</sup> See *id.* at 1176–89 (McKeown, C.J., dissenting).

<sup>85</sup> See *id.* at 1162. Section 230(c)'s grant of immunity applies only if the interactive computer service provider is not also an "information content provider." *Id.* "A website operator can be both a service provider and a content provider: If it passively displays content that is created entirely by third parties, then it is only a service provider with respect to that content. But as to content that it creates itself, or is 'responsible in whole or in part' for creating or developing, the website is also a content provider." *Id.*

<sup>86</sup> 47 U.S.C. § 230(f)(3) (1998) (emphasis added).

<sup>87</sup> See *Roommates.com*, 521 F.3d at 1166. If a subscriber wants to use the website, he has no choice but to answer Roommates.com's questions with one of the responses provided; he may not leave a question blank, nor may he submit an answer that is not in the drop-down menu. See *id.* at 1165. Every profile page was a "collaborate effort between [Roommates.com] and the subscriber" because Roommates.com created the questions and the choice of answers. *Id.* at 1167. In this way, the court suggested, the website was designed to solicit and enforce unlawful housing preferences. See *id.* at 1166.

content that was alleged to violate the Fair Housing Act.<sup>88</sup> The court determined that “[w]hen a business enterprise extracts [unlawful] information from potential customers as a condition of accepting them as clients, it is no stretch to say that the enterprise is responsible, at least in part, for developing that information.”<sup>89</sup>

In reaching its decision, the court adopted a fairly broad definition of “development.”<sup>90</sup> It interpreted the term development as referring “not merely to augmenting the content generally, but to *materially contributing to its alleged unlawfulness*.”<sup>91</sup> The court seemed to indicate that a webhost materially contributes to the alleged illegality of its site if it creates the content itself or if it requires or encourages its users in some way to input the illicit content.<sup>92</sup> In an effort to clarify the standard, the majority provided a few examples of what does, and what does not, amount to development under § 230.<sup>93</sup> On one hand, providing a “neutral tool,” such as a generic search engine, is not development because even though it may be used to carry out illegal searches, the search engine itself does not

<sup>88</sup> See *id.* at 1166. The subscribers to Roommates.com may be considered information content providers because they created their own profiles and picked their own answers from the drop-down menus. See *id.* at 1165. However, the court noted that the website is not necessarily precluded from being treated as an information content provider because the users are also information content providers. See *id.* A website may be liable for making the content available “even if the information originated with a user.” *Id.* at 1166 (citing *Batzel v. Smith*, 333 F.3d 1018, 1033 (9th Cir. 2003)).

<sup>89</sup> *Id.* at 1166. The court further suggested:

The [Federal Housing Act] makes it unlawful to ask certain discriminatory questions for a very good reason: Unlawful questions solicit (a.k.a. “develop”) unlawful answers. Not only does [Roommates.com] ask these questions, [it] makes answering the discriminatory questions a condition of doing business. This is no different from a real estate broker in real life saying, “Tell me whether you’re Jewish or you can find yourself another broker.”

*Id.*

<sup>90</sup> See *id.* at 1167–69 (citing 47 U.S.C. § 230 (f)(3) (noting that “to read the term so broadly would defeat the purpose of *section 230* by swallowing up every bit of the immunity that the section otherwise provides . . . [but] at the same time, reading the exception for co-developers as applying only to content that originates entirely with the website . . . ignores the words ‘development . . . in part’ in the statutory passage ‘creation or development’ in whole or in part”).

<sup>91</sup> *Id.* at 1167–68 (emphasis added). In the dissent, in contrast, Judge McKeown proposed a more narrow definition of development. See *id.* at 1184 (McKeown, C.J., dissenting). She would define “development” as it is defined in the dictionary: “gradual advance or growth through progressive changes.” *Id.* (quoting WEBSTER’S THIRD NEW INTERNATIONAL DICTIONARY 618 (2002)). The majority, however, rejected this definition because it “excludes the kinds of swift and disorderly changes that are the hallmark of growth on the Internet.” *Id.* at 1168. Using the same dictionary, the majority found a definition that was consistent with its understanding of the term and more suitable in the realm of the Internet: “making usable or available.” See *id.* (quoting WEBSTER’S THIRD NEW INTERNATIONAL DICTIONARY 618 (2002)).

<sup>92</sup> See *id.* at 1174. “[T]here is no reason to believe that future courts will have any difficulty applying this principle. The message to website operators is clear: If you don’t encourage illegal content, or design your website to require users to input illegal content, you will be immune.” *Id.* at 1175.

<sup>93</sup> See *Roommates.com*, 521 F.3d at 1169 (elucidating its definition “in an abundance of caution, and to avoid the kind of misunderstanding the dissent seems to encourage”).

contribute to the unlawfulness— the user creates the search on his own terms.<sup>94</sup> On the other hand, however, editing a message in a way that turns an innocent message into an illegal one is development because it clearly contributes to the unlawfulness of the content.<sup>95</sup> The court resolved that Roommates.com's activities fell into the latter category of cases because its questions and answers forced users to enter responses that would be used for discriminatory purposes in the sale or rental of housing, thereby directly and materially contributing to the unlawfulness of the postings.<sup>96</sup> In so holding, the court imposed an unprecedented expansion of liability and essentially uprooted the traditional notion of robust immunity for website providers under § 230.

### III. THE REPERCUSSIONS OF IMMUNITY UNDER § 230

The extent of Internet service provider immunity under § 230 implicates competing public policy concerns. At one end of the spectrum is the fear that anything less than absolute immunity will threaten the growth and development of the Internet. At the other end, however, is the concern that complete and expansive immunity jeopardizes the private person's right to be free from discrimination, defamation, invasion of privacy, and other wrongful conduct because it creates a disincentive for website providers to act as responsibly as possible. The following sections consider the arguments with respect to the degree of § 230 immunity in turn.

#### A. A Case for Expansive Immunity

Some legal scholars take the position that granting robust immunity for website providers is the best, and perhaps only, way to protect the expanding landscape of cyberspace and to encourage the free exchange of ideas.<sup>97</sup> One very specific argument is that imposing liability on Internet

<sup>94</sup> See *id.* Google, for example, does not “develop” illegal content simply because a user might use it to search: looking for a “white roommate.” *Id.*; see also 47 U.S.C. § 230 (f)(3). “The term ‘information content provider’ means any person or entity that is responsible, in whole or in part, for the creation or development of information provided through the Internet or any other interactive computer service.” *Id.*

<sup>95</sup> See *Roommates.com*, 521 F.3d at 1169 (citing as an example of this situation where a website provider removes the word “not” from a user’s message reading “[Name] did *not* steal the artwork”); see also *Batzel v. Smith*, 333 F.3d 1018, 1034 (9th Cir. 2003) (suggesting that an editors’ grammatical corrections and posting of a third parties letter did not contribute to the unlawfulness of the content).

<sup>96</sup> See *Roommates.com*, 521 F.3d at 1172 (explaining that Roommates.com went beyond providing mere neutral tools that could be utilized for proper or improper purposes); see also *Goddard v. Google, Inc.*, 640 F. Supp. 2d 1193, 1198 (N.D. Cal. 2009) (suggesting that Roommates.com elicited “the allegedly illegal content” and made “aggressive use of it in conducting its business”).

<sup>97</sup> The individuals espousing this view generally support broad immunity under § 230 because

service providers will ultimately “[diminish] the value and promise” of the new interactive online world.<sup>98</sup> This argument flows from the belief that the Internet is valuable because low barriers of entry<sup>99</sup> provide the masses with “unprecedented power to access, create, and publish.”<sup>100</sup> Internet users can share intelligence and actively create content for widespread public view,<sup>101</sup> and it is precisely from this diverse range of human input that the Internet gains its value and “vast social utility.”<sup>102</sup> As a corollary, the Internet would lose that value if input were to be constrained.<sup>103</sup> Thus, because extending liability would limit input by effectively forcing Internet service providers to edit and filter content,<sup>104</sup> those individuals concerned with preserving the Internet’s value argue that there can be no alternative to absolute immunity.<sup>105</sup>

Another argument in favor of maintaining a judicial policy of robust immunity is that any effort to expand liability will forcibly chill free speech and the “robust development of the Internet” by creating substantial

Congress passed the act with a view towards accomplishing these very goals. For example, Cecilia Ziniti endorses a broad interpretation of § 230 immunity because it “[effectuates] Congressional intent to ‘promote the continued development of the Internet and other interactive computer services.’” See Ziniti, *supra* note 43, at 610.

<sup>98</sup> *Id.* at 595.

<sup>99</sup> See *id.* at 591 (stating that “[a]nyone with access to a public library can access the Internet”); see also Oren Bracha & Frank Pasquale, *Federal Search Commission? Access, Fairness, And Accountability In The Law Of Search*, 93 CORNELL L. REV. 1149, 1155 (2008) (suggesting that because the internet has high accessibility and value because of its low barrier of entry).

<sup>100</sup> Ziniti, *supra* note 43, at 591.

<sup>101</sup> See *id.* at 590 (contrasting the current landscape of the Internet with the earlier model, where users used “static directories” and “observed, found, and exchanged content passively” and privately); see also *ACLU v. Reno*, 521 U.S. 844, 850 (1997) (stating that the Internet allows millions of people “to communicate with one another and to access vast amounts of information from around the world”).

<sup>102</sup> See Ziniti, *supra* note 43, at 591. In her article, Ziniti argues that the “network effect” is even more powerful in the new, more interactive Internet than it was before. *Id.* at 593. She explains the “network effect” as the notion that “the value of a network to a given customer depends on the numbers of users of it.” *Id.* (citing Posting of Bob Metcalfe to VCMike’s Blog, Metcalfe’s Law Recurses Down the Long Tail of Social Networking, <http://vc-mike.wordpress.com/2006/08/18/metcalfe-social-networks/> (Aug. 18, 2006)). Thus, as a result of the network effect, restricting human input would necessarily destroy the value of the Internet “exponentially.” *Id.*

<sup>103</sup> See *id.*; see also James M. McGee, *Recent Development: Burning the Village to Roast the Pig: Congressional Attempt to Regulate “Indecency” on the Internet Rejected in ACLU v. Reno*, 4 J. INTELL. PROP. L. 437, 462 (1997) (“[T]he negative consequences of restricting speech on the Internet through the CDA are enormous . . . The strength of the Internet lies in its diversity of content due to a large number of participants from a variety of backgrounds with easy access to the Internet.”).

<sup>104</sup> See Ziniti, *supra* note 43, at 594; see also *Batzel v. Smith*, 333 F.3d 1018, 1027–28 (9th Cir. 2003) (explaining that “[m]aking interactive computer services and their users liable for the speech of third parties would severely restrict the information available on the Internet”).

<sup>105</sup> See Ziniti, *supra* note 43, at 583 (opining that a wide grant of immunity under § 230 is “constitutionally, practically, and socially preferable to [any] alternatives – especially as applied to the new landscape of online services”); see also *Roommates.com*, 521 F.3d at 1177 (McKeown, C.J., dissenting) (indicating that “there should be a high bar to liability for organizing and searching third-party information”).



uncertainty about the rules for website providers.<sup>106</sup> Absent a bright line rule, a webhost will not have the comfort of knowing that he is immune under § 230 for third-party postings.<sup>107</sup> Accordingly, if a website provider knows that he may potentially face liability for publishing user-generated messages, he may “restrict or abandon many of the features that enable the dissemination of third-party content.”<sup>108</sup> This is especially true where the website carries a “staggering volume of third-party content.”<sup>109</sup> Thus, because imposing liability may cause an operator to limit the scope of his website’s services on the side of caution, it can hardly be said to encourage the “vibrant and competitive free market” on the Internet.<sup>110</sup>

A final argument in favor of expansive immunity is that Congress simply intended broad immunity as the means to achieve its policy goals.<sup>111</sup> In her dissent in *Roommates.com*, Judge McKeown suggested that Congress clearly purported to create a “high bar” to liability for organizing user-generated content on the Internet even though traditional information providers did not have immunity for similar editing functions.<sup>112</sup> The Internet was distinguished from other media because it represented a new form of communication with “unique opportunities for cultural

<sup>106</sup> See *Zeran*, 129 F.3d at 331 (“The specter of tort liability in an area of such prolific speech would have an obvious chilling effect.”); see also Brief for Amazon.com, Inc. et al. as Amici Curiae Supporting Defendant-Respondent at 4, Fair Hous. Council of San Fernando Valley v. *Roommates.com*, LLC, 521 F.3d 1157 (9th Cir. June 15, 2005) (Nos. 04-56916, 04-57173), 2005 U.S. 9th Cir. Briefs LEXIS 442, 8 (explaining that because the vitality of the Internet depends in part on the ability to avoid liability for content created by one of the millions of third-party users, imposing liability would create uncertainty among website providers and thus “imperil the future growth” of the online community).

<sup>107</sup> See *Roommates.com*, 521 F.3d at 1177 (McKeown, C.J., dissenting) (indicating that the majority’s proposed standard for imposing liability “offers interactive computer service providers no bright lines and little comfort in finding a home within § 230(c)(1)”).

<sup>108</sup> Brief for Amazon.com, Inc. et al. as Amici Curiae, *supra* note 106, at 31.

<sup>109</sup> See *id.*; see also *Zeran*, 129 F. 3d at 331 (noting that website providers might be forced to “severely restrict the number and type of messages posted” because it would be “impossible for service providers to screen each of their millions of postings for possible problems”).

<sup>110</sup> See 47 U.S.C. § 230(b)(2) (1996) (identifying preserving the “vibrant and competitive free market” unfettered by regulation as one of the express policies of Congress).

<sup>111</sup> See Brief for Amazon.com, Inc. et al. as Amici Curiae, *supra* note 106, at 32 (arguing that an interpretation of § 230, such as the one proposed by Fair Housing Council in *Roommates.com*, that tends to expand the liability of website providers for third-party content “contravenes [the] express Congressional goal”); see also *Batzel*, 333 F.3d at 1027 (stating that Congress made the legislative choice to provide immunity to advance its policy objective of encouraging “the unfettered and unregulated development of free speech on the Internet, and to promote the development of e-commerce”).

<sup>112</sup> See *Roommates.com*, 521 F.3d at 1177 (McKeown, C.J., dissenting) (“[T]he anomaly that a webhost may be immunized for conducting activities in cyberspace that would traditionally be cause for liability is *exactly what Congress intended* by enacting [§ 230].”) (emphasis added); see also 800-JR Cigar, Inc. v. GoTo.com, Inc., 437 F. Supp. 2d 273, 295 (D.N.J. 2006) (“The purpose of [§230] is to promote self-regulation of Internet service providers. Basically, the [legislation] shields service providers from liability for the content of websites of third parties that are accessed through the Internet.”).

development.”<sup>113</sup> Congress recognized the need to facilitate its development<sup>114</sup> and thus “chose[] to treat cyberspace differently.”<sup>115</sup> The courts have understood this to mean that Congress intended to grant expansive immunity, and in the past six years, Congress has not expressed any disapproval with that interpretation.<sup>116</sup> Accordingly, some of those in favor of broad immunity rely on this approval to support the decision to “stay the course of ‘robust’ webhost immunity.”<sup>117</sup>

### *B. A Case for Limited Immunity*

In response to this zealous support for expansive immunity, a number of scholars contend that a scheme of more limited immunity under § 230 is appropriate and potentially necessary. One consideration underlying this view is the effect that blanket immunity for Internet service providers may have on the private individual.<sup>118</sup> These scholars argue that § 230 does a “true disservice” to private individuals harmed on the Internet because when website provider immunity is coupled with the fact that most Internet users are anonymous, the chance of recovery shrinks.<sup>119</sup> When comments

<sup>113</sup> See § 230(a)(3). Congress also found that the Internet offered a “forum for a true diversity of . . . discourse” and “myriad avenues for intellectual activity.” *Id.*

<sup>114</sup> See *Roommates.com*, 521 F.3d at 1187 (McKeown, C.J., dissenting) (arguing that Congress explicitly drafted the law to permit unfettered development); see also § 230(b)(2) (articulating the United States’ policy to preserve the vibrant Internet market “unfettered by Federal or State regulation”).

<sup>115</sup> See *Batzel*, 333 F.3d at 1027. The District Court for the District of Columbia further underscored Congress’s intention to provide different treatment for website providers:

In recognition of the speed with which information may be disseminated and the near impossibility of regulating information content, Congress decided not to treat providers of interactive computer services like other information providers such as newspaper magazines or television and radio stations, all of which may be held liable for publishing or distributing obscene or defamatory material written or prepared by others.

*Blumenthal v. Drudge*, 992 F. Supp. 44, 49 (D.D.C. 1998).

<sup>116</sup> See *Metrosplash.com*, 339 F.3d at 1123 (noting that “courts have treated §230(c) immunity as quite robust, adopting a relatively expansive definition of ‘interactive computer service’ and a relatively restrictive definition of ‘information content provider’”); see also *Roommates.com*, 521 F.3d at 1187 (McKeown, C.J., dissenting) (expressing the idea that “[h]ad Congress discovered that, over time, courts across the country have created more expansive immunity than it originally envisioned under [§ 230], Congress would have amended the law”).

<sup>117</sup> *Roommates.com*, 521 F.3d at 1188.

<sup>118</sup> See generally Langdon, *supra* note 25 (arguing that § 230 effectively deprives the private individual of adequate legal remedies); see also Sheridan, *supra* note 32, at 150 (discussing how §230 bars people who have been defamed from recovering from the large service providers who may have contributed to the damages).

<sup>119</sup> See Langdon, *supra* note 25, at 854 (suggesting that user anonymity and service provider immunity may force attorneys to advise their clients against filing defamation claims); see also Sewali K. Patel, *Immunizing Internet Service Providers from Third-Party Internet Defamation Claims: How Far Should Courts Go?*, 55 VAND. L. REV. 647, 688 (2002) (explaining that “[p]roviding a blanket immunity to [internet service providers] may have the negative consequence of wiping out the existence of tort defamation claims altogether in the Internet context”).

are made anonymously, individuals are left with very few, if any, avenues for recovery.<sup>120</sup> Even when comments are not made anonymously, however, the private individual is still denied an adequate opportunity for redress because he is prohibited from going after deep-pocket companies, such as America Online or Microsoft Network.<sup>121</sup>

Another argument in favor of limiting the scope of immunity under § 230 is that absolute blanket immunity gives very little incentive for Internet service providers to take responsibility for the material on their website.<sup>122</sup> One of Congress's purposes behind enacting § 230 was to encourage the website providers to "self-regulate the dissemination of offensive material over their services."<sup>123</sup> Yet absolute immunity is entirely inconsistent with a goal of self-regulation because an Internet service provider will have no incentive to self-regulate if he knows that he will be immune from liability regardless of whether or not he polices the content on his website.<sup>124</sup> Thus,

<sup>120</sup> The trend appears to be to sue the Internet service provider in lieu of the anonymous commentator – even though the provider will most likely be deemed immune. *See, e.g., Metrosplash.com*, 339 F.3d at 1122. In a recent case that is attracting a lot of media attention, however, two females filed a lawsuit against 40 anonymous website posters using their screennames. *See* Christian Nolan, *Yale Law School defamation case explores anonymous Website users' free speech rights*, CONN. L. TRIB., Mar. 26, 2008, available at <http://www.law.com/jsp/nlj/PubArticleNLJ.jsp?id=1206441805828>. The plaintiffs issued a subpoena for information relating to "AK47," one of the anonymous individuals responsible for making sexually explicit comments about them. *See Doe I v. Individuals*, 561 F. Supp. 2d 249, 250 (D. Conn. 2008). The defendant moved to quash the subpoena on the ground that disclosure of his identity would violate his First Amendment right to engage in anonymous speech. *See id.* at 253. In a decision that shocked a number of individuals in the legal community, the court denied the motion to quash, finding that the plaintiff's interest in pursuing discovery in the case outweighed the defendant's First Amendment right to speak anonymously. *See id.* at 257. In response to the identification of "AK47," Ryan Singel commented: "The unmasking of the posters marks a milestone in a rare legal challenge to the norms of online commenting[.]" Ryan Singel, *Yale Students' Lawsuit Unmasks Anonymous Trolls, Opens Pandora's Box*, WIREd, July 30, 2008, <http://www.wired.com/politics/law/news/2008/07/autoadmit> (emphasis added). This suggests that plaintiff's attempt to uncover the identity of the anonymous poster was somewhat exceptional.

<sup>121</sup> *See* Patel, *supra* note 119, at 661 (noting that "since the CDA's enactment in 1996, there has not yet been a single case that has held an [internet service provider] liable for disseminating third-party defamatory statements over the Internet"); *see also* Sheridan, *supra* note 32, at 149 (explaining that mandating immunity under § 230 "denies individuals whose reputations have been damaged any recovery against even the largest corporations whose malfeasance or nonfeasance contributed to the damage").

<sup>122</sup> *See* Langdon, *supra* note 25, at 848 (suggesting that "[b]y allowing virtually total immunity in defamation actions, section 230(c)(1) creates no incentive for Internet providers to remove defamatory material"); *see also* Patel, *supra* note 119, at 678 (discussing that a "problem created by the blanket immunity provided to [internet service providers] is that it has left no incentive for [internet service providers] to monitor or edit their content").

<sup>123</sup> *See Zeran*, 129 F.3d at 331; *see also* 47 U.S.C. § 230(b)(3) (1996) (stating that "[i]t is the policy of the United States . . . to encourage the development of technologies which maximize user control over what information is received by individuals, families, and schools who use the Internet and other interactive computer services").

<sup>124</sup> *See* Langdon, *supra* note 25, at 855 (remarking that the only incentive for website providers to remove libelous material is to improve customer relations); *see also* David L. Hudson Jr., *Taming the Gossipmongers*, 94 A.B.A.J. (forthcoming July 2008), available at [http://abajournal.com/magazine/taming\\_the\\_gossipmongers](http://abajournal.com/magazine/taming_the_gossipmongers) (quoting Daniel Solove, a law professor, explaining that § 230 has "been

“[t]he net effect of [§ 230] is to give free reign to the Internet companies to do whatever they please.”<sup>125</sup> To avoid this result, scholars propose removing the safety net of absolute immunity, thereby encouraging website providers to act responsibly to avoid liability.<sup>126</sup>

Finally, some scholars argue against robust immunity because they are not entirely convinced that Congress intended such sweeping protection.<sup>127</sup> The argument is that broad immunity should not “be inferred by a court from a statute that does not explicitly confer it[.]”<sup>128</sup> Expansive immunity for website providers may appear consistent with the intent to promote free and dynamic communication on the Internet, but that does not necessarily mean that Congress purported to grant it in § 230.<sup>129</sup> In fact, granting blanket immunity to service providers who permit unlawful or defamatory activity in the name of “promoting free speech” is inconsistent with the authority of First Amendment law. The Supreme Court has held that although the First Amendment prohibits legislation against free speech, it “cannot have been, and obviously was not, intended to give immunity for every possible use of language.”<sup>130</sup> In other words, even where free speech is implicated, absolute immunity does not exist.<sup>131</sup> In light of this principle, it is more likely that Congress did not intend to grant blanket immunity for

turned into a blanket immunity that allows sites to leave up content that they know is defamatory or invasive of privacy”).

<sup>125</sup> Langdon, *supra* note 25, at 848.

<sup>126</sup> See *id.* at 854–55 (suggesting that the courts extend liability to Internet providers in situations where they are placed on notice that they are distributing defamatory material, effectively forcing website providers to “assume some responsibility for the materials that pass through their services” without undermining Congress’s goal to promote the development of the Internet); see also Sheridan, *supra* note 32, at 179 (questioning whether immunity is necessary and noting that it “creates an asymmetry between electronic and print media that is difficult to justify”).

<sup>127</sup> See Sheridan, *supra* note 32, at 151 (“[B]road immunity represents a value judgment not to be made lightly by Congress[.]”); see also Jae Hong Lee, Batzel v. Smith & Barrett v. Rosenthal: *Defamation Liability for Third-party Content on the Internet*, 19 BERKELEY TECH. L.J. 469, 474 (2004) (“[I]t seems reasonable to assume that if Congress had wanted to grant immunity from distributor liability, it would have done so explicitly.”).

<sup>128</sup> Sheridan, *supra* note 32, at 151 (arguing that “until Congress acts more clearly, courts should continue to resolve cases involving alleged distributor liability according to traditional tort principles”).

<sup>129</sup> See *id.* at 178 (noting that although freedom from distributor liability might be necessary to “preserve the ‘never-ending worldwide conversation’” on the Internet, there is little evidence that Congress made the choice to grant it in enacting § 230 (quoting *ACLU v. Reno*, 929 F. Supp. 824, 883 (E.D. Pa. 1996)); see also Lee, *supra* note 127, at 493 (stating that the narrower construction of *Barrett v. Rosenthal* is probably more consistent with Congress’ original intent and would make amendments by Congress unnecessary to end distributor immunity from liability).

<sup>130</sup> *Frohwerk v. United States*, 249 U.S. 204, 206 (1919).

<sup>131</sup> See, e.g., *Virginia v. Black*, 538 U.S. 343, 358 (2003) (noting that the protections afforded by the First Amendment are “not absolute, and [the Court has] long recognized that the government may regulate certain categories of expression consistent with the Constitution”); see also *Chaplinsky v. New Hampshire*, 315 U.S. 568, 571–72 (1942) (explaining that “[t]here are certain well-defined and narrowly limited classes of speech, the prevention and punishment of which has never been thought to raise any Constitutional problem”).

service providers under § 230.

This final argument suggesting that Congress did not intend to grant absolute immunity stands in stark opposition to the argument supporting broad immunity on the ground that Congress clearly intended it as the means to achieve its policy goals.<sup>132</sup> Thus, it is no wonder that the courts have started to disagree on the meaning of § 230 and question the extent to which Congress intended website providers to be immune from liability.

#### IV. LIMITING IMMUNITY AS A MEANS TO PROMOTE RESPONSIBILITY AMONG INTERNET SERVICE PROVIDERS AND PROTECT THE PRIVATE INDIVIDUAL

This section argues that a narrower interpretation of the extent of § 230 immunity provides a superior alternative to blanket immunity. Blanket immunity frustrates the congressional goals of encouraging self-regulation and promoting the useful exchange of information on the Internet. Imposing a scheme of liability, however, is consistent with the policies behind § 230. First, it will induce website providers to self-regulate and act more responsibly in overseeing the content on their website, thereby protecting the private person's right to be free from discrimination, defamation, and invasion of privacy. Second, it will ensure that service providers are in fact promoting the exchange of useful and valuable information, rather than allowing the dissemination of illegal and harmful speech.

##### *A. Effectuating the Congressional Goals of § 230 through a Scheme of Limited Liability*

One of the unfortunate consequences of the "vibrant and competitive free market"<sup>133</sup> on the Internet is that it threatens the individual's ability to protect his reputation from unwarranted damage.<sup>134</sup> The Internet is "the most participatory form of mass speech yet developed."<sup>135</sup> It provides

<sup>132</sup> See *supra* notes 111–17 and accompanying text.

<sup>133</sup> 47 U.S.C. § 230(b)(2) (1996).

<sup>134</sup> See SOLOVE, *supra* note 12, at 30. Solove claims that because information can spread so easily and quickly, there will be "more instances when information we want to keep on a short leash will escape our control." *Id.* at 29. Once this information finds "its way into the minds of others, we can't control what they think about it." *Id.* at 35. A person's reputation depends on how others make judgments about the information they receive. *Id.* at 33. Thus, Solove argues that the unbridled "proliferation of personal data" on the Internet may severely compromise a person's good reputation. *Id.* at 30. This is worsened by the relative anonymity and ease of publishing on the Internet. Lee, *supra* note 127, at 471–72.

<sup>135</sup> *ACLU v. Reno*, 929 F. Supp. at 883.

nearly instant access to a wealth of information and facilitates a large-scale exchange of views and ideas. The cost of this “never-ending worldwide conversation,”<sup>136</sup> however, is that it offers “an unprecedented means for irresponsible individuals to cause damage by propagating false and defamatory statements around the world at the speed of light.”<sup>137</sup> Even personal photographs and accurate information may “[spread] around the Internet like a virus,” violating a person’s right to privacy.<sup>138</sup> Regrettably, the private individual’s injury from Internet gossip is exacerbated by the fact that the “fragments of information won’t [sic] fade away with time.”<sup>139</sup> Information in Cyberspace is “permanent and searchable.”<sup>140</sup>

To curb the amount of harmful and illegal content, there must be some incentive for Internet service providers to keep a more watchful eye over the content on their websites. Guaranteeing webhosts immunity under § 230 is not the most effective means of accomplishing this goal because it rewards a website operator who knowingly ignores offensive third-party content with the same protection that it rewards a webhost who zealously combs through user-generated posts.<sup>141</sup> Thus, absolute immunity is inconsistent with the congressional goal of self-regulation. If, on the other

<sup>136</sup> *Id.*

<sup>137</sup> See Sheridan, *supra* note 32, at 151; see also Singel, *supra* note 120 (suggesting that the Internet is a place where “reputations can be sullied nearly irreparably by anyone with a grudge, a laptop and a WiFi connection”).

<sup>138</sup> See SOLOVE, *supra* note 12, at 2. Professor Solove laments some of the terrifying implications from the flow of information on the Internet. He explains the new phenomenon taking place on the Internet:

We can now readily capture information and images wherever we go, and we can then share them with the world at the click of a mouse. Someone you’ve never met can snap your photo and post it on the Internet. Or somebody that you know very well can share your cherished secrets with the entire planet. Your friends or coworkers might be posting rumors about you on their blogs. The personal email you send to others can readily be forwarded along throughout cyberspace, to be mocked and laughed at far and wide.

*Id.* Solove suggests that gossip on the Internet is worse than typical “water cooler gossip” because it transforms gossip into “a widespread and permanent stain on people’s reputations.” *Id.* at 181. Thus, he suggests publishing gossip online, even if only among a few people, should still be considered a violation of privacy. *Id.*

<sup>139</sup> See *id.* at 2; see also Singel, *supra* note 120 (noting that online postings “live on for years in search-engine results”).

<sup>140</sup> See SOLOVE, *supra* note 12, at 4. Solove further notes that historically, written gossip has been considered more harmful than oral gossip. *Id.* at 181. This is especially true, he suggests, of gossip written on the Internet. *Id.* He explains that Internet rumor can spiral out of control because “[e]ven if [information] is posted on an obscure blog, [it] can still appear in a Google search under a person’s name.” *Id.*

<sup>141</sup> See *Zeran v. America Online, Inc.*, 129 F.3d 327, 330, 331 (4th Cir. 1997) (explaining that, as an incentive to self-regulate, Congress bars any claims against an Internet service provider for publishing, withdrawing, or altering content); see also *Blumenthal v. Drudge*, 992 F. Supp. 44, 52 (D.D.C. 1998) (noting that Congress, “[i]n some sort of tacit *quid pro quo* arrangement with the service provider community . . . has conferred immunity from tort liability as an incentive to Internet service providers to self-police the Internet for obscenity and other offensive material, even where the self-policing is unsuccessful or not even attempted.”).

hand, the statute imposed liability on webhosts for certain illegal or tortious user content, those webhosts would be more likely to reconsider the option of screening such content in order to avoid a lawsuit.

The major concern behind forcing Internet service providers to police third-party material is that it undermines the express Congressional policies behind § 230. Imposing liability in certain limited circumstances, however, will still effectuate the two goals set by Congress. First, Congress endeavored to encourage self-regulation among Internet service providers.<sup>142</sup> Imposing liability clearly advances this goal because, as indicated above, the paramount purpose behind imposing liability is to create incentives for webhosts to act more responsibly and monitor user-generated posts. Second, Congress purported to “promote the continued development of the Internet”<sup>143</sup> and preserve the “robust nature of Internet communication.”<sup>144</sup> A scheme of limited liability tailored to protect the private individual from damaging speech on the Internet would be perfectly consistent with these objectives because it would not interfere with the dissemination of valuable and useful information and ideas. On the contrary, it would only stifle the publication of harmful, illegal or tortious commentary. Such material has no value in the eyes of the law<sup>145</sup> and thus contributes very little, if anything, to the “vibrant and competitive free market” of the Internet.<sup>146</sup> In effect, the Internet’s growth in size and in value would be uninterrupted by efforts to encourage website providers to delete injurious content. Therefore, a policy of affording immunity to service providers who promote unlawful communication that is neither valuable nor useful undermines the goal of preserving a vibrant free market under § 230(b)(2) more seriously than a policy of limited liability.

<sup>142</sup> See *Fair Hous. Council of San Fernando Valley v. Roommates.com, LLC*, 521 F.3d 1157, 1175 (9th Cir. 2008) (stating that the intent, under § 230, is to encourage service providers’ self-policing of content without fear of liability for every message posted by third parties); see also *Zeran*, 129 F.3d at 331 (explaining that immunizing service providers furthers the purpose of encouraging self-regulation by eliminating the fear of liability traditionally attached to publishers that regulate offensive material).

<sup>143</sup> 47 U.S.C. § 230(b)(1) (1996).

<sup>144</sup> *Zeran*, 129 F.3d at 330.

<sup>145</sup> See, e.g., *Gertz v. Robert Welch, Inc.*, 418 U.S. 323, 340 (1974) (reasoning that since false statement of facts have no constitutional value, they are not accorded constitutional protection); *Dennis v. United States*, 341 U.S. 494, 544 (1951) (Frankfurter, J., concurring) (asserting that different types of speeches occupy different levels on the value scale, and that there may be no public interest in protecting certain speeches).

<sup>146</sup> See § 230(b)(2). One of the purposes of Congress is to preserve this “vibrant and competitive free market that presently exists for the Internet.” *Id.* Importantly, Congress explicitly states that is its policy “to ensure vigorous enforcement of Federal criminal laws to deter and punish trafficking in obscenity, stalking, and harassment by means of computer.” *Id.* at (b)(5). This seems to underscore the notion that Congress did intend to eliminate certain illegal acts and statements from the landscape of the Internet. Thus it is clear that not all content is valuable in cyberspace.

Importantly, in addition to immunizing harmful speech that does not contribute to the Internet's value, a scheme of absolute immunity would also immunize speech that may otherwise be punishable. The Supreme Court has recognized that the First Amendment does not grant absolute immunity for all classes of speech.<sup>147</sup> Indeed, the Constitution permits the government to regulate certain limited uses of the language.<sup>148</sup> For example, the First Amendment guarantee of freedom of speech does not protect "true threats,"<sup>149</sup> "fighting words,"<sup>150</sup> or other utterances which may provoke a breach of the peace.<sup>151</sup> Likewise, the First Amendment allows states to punish "the lewd and obscene, the profane, [and] the libelous."<sup>152</sup> Such communication, which is prohibited in the real world, should also be prohibited in Cyberspace; to allow otherwise would be inconsistent with the authority of First Amendment law.<sup>153</sup> Granting absolute immunity to service providers who promote such speech would have the effect of condoning unlawful utterances. Imposing liability, on the other hand, would ensure that the unprotected speech does not become permissible simply because it is disseminated on the Internet. As evidenced by its stated policy to enforce criminal laws "to deter and punish trafficking in obscenity, stalking, and harassment by means of

<sup>147</sup> See *Virginia v. Black*, 538 U.S. 343, 358 (2003) (commenting that the government may constitutionally regulate certain types of expression); see also *R.A.V. v. City of St. Paul*, 505 U.S. 377, 382–83 (1992) (expressing that society has accepted limitations on free speech in situations where the benefit of the speech is minimal when compared to the social interest in maintaining morality, and that First Amendment protections cannot offend such limitations).

<sup>148</sup> See *R.A.V.*, 505 U.S. at 382–83 (stating that the government has "permitted restrictions upon the content of speech in a few limited areas, which are 'of such slight social value as a step to truth that any benefit that may be derived from them is clearly outweighed by the social interest in order and morality'" (quoting *Chaplinsky v. New Hampshire*, 315 U.S. 568, 572 (1942))). See also *Dennis*, 341 U.S. at 503 (suggesting that sometimes the societal value of free speech must give way to other considerations).

<sup>149</sup> See *Watts v. United States*, 394 U.S. 705, 708 (1969) (indicating that a true threat is not protected under the First Amendment, and holding that the petitioner's statements could not be construed as a true threat).

<sup>150</sup> See *Cohen v. California*, 403 U.S. 15, 20 (1971) (noting that that states are free to ban the use of "personally abusive epithets which, when addressed to the ordinary citizen, are, as a matter of common knowledge, inherently likely to provoke violent reaction").

<sup>151</sup> See *Schenck v. United States*, 249 U.S. 47, 52 (1919) ("The most stringent protection of free speech would not protect a man in falsely shouting fire in a theater and causing a panic.").

<sup>152</sup> See *Chaplinsky v. New Hampshire*, 315 U.S. 568, 572 (1942); see also *Garrison v. Louisiana*, 379 U.S. 64, 75 (1964) (stating that "[a]lthough honest utterance, even if inaccurate, may further the fruitful exercise of the right of free speech, it does not follow that the lie, knowingly and deliberately published about a public official, should enjoy a like immunity").

<sup>153</sup> See *Sheridan*, *supra* note 32, at 179 (concluding that "construing 230 to immunize services from distributor liability creates an asymmetry between electronic and print media that is difficult to justify"); Peter J. Breckheimer II, *A Haven for Hate: The Foreign and Domestic Implications of Protecting Internet Hate Speech Under the First Amendment*, 75 S. CAL. L. REV. 1493, 1507 (2002) (indicating that it is within the government's power to regulate hate speech on the internet).



computer,”<sup>154</sup> Congress clearly did not intend to make all types of Internet communication and activity lawful. Because a scheme of limited liability would effectuate this policy and comport with the great authority of First Amendment law, it appears to be the better alternative.

### *B. Delineating a Proper Standard for Imposing Liability*

Because a narrower interpretation of the scope of immunity under § 230 is consistent with the Congressional objective and the authority of First Amendment law, the argument that Congress clearly intended broad immunity as the *only* means to achieve its policy goals<sup>155</sup> is unpersuasive. Therefore, the statute should not be understood as granting absolute blanket immunity to website providers. What remains to be decided, however, is when, and under what specific circumstances, liability should attach.

The decision in *Roommates.com* is a step in the right direction to the extent that it attempts to limit robust immunity under § 230. Be that as it may, the standard that the court applied is inadequate to ensure that the proper Internet service providers face liability. In *Roommates.com*, the court proposed that the decisive factor in determining the availability of immunity should be whether the webhost was a content provider. It concluded that Internet providers who “[contribute] materially to the alleged illegality” of the information on their website are content providers, and thus do not qualify for immunity under § 230.<sup>156</sup> Service providers, the court decided, were eligible to receive the full extent of § 230 protection.<sup>157</sup>

The fundamental problem with the *Roommates.com* standard is that it is too vague to guarantee that courts will impose liability uniformly and fairly. “Contributing materially” to the unlawfulness of content could encompass a great number of activities, some of which may not warrant the imposition of liability. Consider, for example, the theoretical celebrity gossip forum discussed in the Introduction. The webhost appeared to be a service provider because he simply created the forum; he did not contribute to any discussions or supervise the activities of the third-party users. A court could find, however, that he materially contributed to the unlawfulness of the user-generated content by virtue of the fact that his forum was designed to “encourage illegal content,”<sup>158</sup> namely defamatory

<sup>154</sup> 47 U.S.C. § 230(b)(5) (1996).

<sup>155</sup> See *supra* notes 111–17 and accompanying text.

<sup>156</sup> *Roommates.com*, 521 F.3d. at 1168.

<sup>157</sup> See *id.* at 1162 (noting that § 230’s broad grant of immunity applies “only if the interactive computer service provider is not also an ‘information content provider’”).

<sup>158</sup> See *id.* at 1175 (indicating that a webhost materially contributes to the illegality of his website

gossip about celebrities.

A proper standard for determining when a website provider is immune under § 230 should not hinge on the tenuous inquiry of whether the webhost's activities amounted to creation or development of information. Instead, the courts should focus on the extent to which the Internet service provider was, or should have been, aware of the possible ramifications of his website. In other words, the courts should consider whether the particular nature of the website was such that it should have put the webhost on notice of the possibility for unlawful third-party posting. If it is reasonably clear that the website, by virtue of its subject matter or design, is likely to elicit illegal or tortious content, the website operator should be held to a higher standard of care with respect to screening user-generated information. If, however, it is highly unlikely that the website will yield objectionable material, the operator will have a lesser degree of care and a stronger presumption of immunity.

The method for applying this proposed standard is clear-cut. The courts should simply base their determination of the website's risk for illegal content on two criteria: the inherent subject matter of the website and the vehicle through which it collects third-party postings. Consider, for example, the website in *Roommates.com*.<sup>159</sup> In that case, it should have been extremely clear to the webhost that his site was likely to elicit illegal information because he made it possible for users to select unlawful discriminatory responses by providing them in the drop-down menu in the first place.<sup>160</sup> Thus, the specific vehicle through which *Roommates.com* gathered the user-generated content should have put the webhost on notice of the likelihood of unlawful postings. In *Carafano*, on the other hand, the webhost had no reason to believe that his users would post tortious statements. In that case, the website was simply a dating website that allowed users to create profiles containing descriptive information about their age, appearance, interests, and personality for the purpose of meeting someone.<sup>161</sup> Individuals do not typically join these match-making communities for the purpose of making false and sexually explicit profiles about celebrities.<sup>162</sup> Therefore, the subject matter of the website was not of

if he "[encourages] illegal content, or [designs his] website to require users to input illegal content").

<sup>159</sup> In this case, the website was "designed to match people renting out spare rooms with people looking for a place to live." *See id.* at 1161.

<sup>160</sup> *See id.* at 1165.

<sup>161</sup> *See Carafano v. Metroplash.com*, 339 F.3d at 1121.

<sup>162</sup> *See id.*; see also Jeffrey Lipschutz, *Internet Dating . . . Not Much Protection Provided by the Communications Decency Act of 1996 Based on Carafano v. Metroplash.com*, 339 F.3D 1119 (9th Cir. 2003), 23 TEMP. ENVTL. L. & TECH. J. 225, 228 (2004) (discussing the safeguards of

a nature that would have indicated to the webhost a great risk of tortious third-party postings.

### CONCLUSION

The Internet is undoubtedly a valuable tool. This value, however, is coming at a high price to the very people it is intended to benefit – the private individuals. Interpreting § 230 as providing robust blanket immunity to webhosts is problematic insofar as it does not provide any incentives for interactive computer service providers to carefully monitor user-generated posts for possible tortious or illegal content. As a result, the private individual is seriously limited in his ability to protect himself from discrimination, defamation, invasions of privacy, and other unlawful attacks. Therefore, a narrower interpretation of § 230 is preferable. Imposing liability under certain limited circumstances will induce webhosts to take more responsibility for the content on their websites. Moreover, it is perfectly consistent with the Congressional policies behind § 230, namely, to promote the exchange of valuable information and to encourage the self-regulation of Internet service providers. In order to ensure that the courts impose liability fairly and coherently, the standard should not hinge on the tenuous distinction between content providers and service providers. Rather, the standard should focus on the extent to which the webhost was, or should have been, aware of the risk of illicit or tortious third-party postings. Under this standard, Cyberspace will continue to flourish – but its growth will not come at the expense of the millions of Internet users.