"INDECENT" DECEPTION: THE ROLE OF COMMUNICATIONS DECENCY ACT § 230 IN BALANCING CONSUMER AND MARKETER INTERESTS ONLINE

Amy J. Tindell

"[T]he Internet represents a brave new world of free speech ... [it] is fundamentally different from traditional forms of mass communication in at least three important respects. First, the Internet is capable of maintaining an unlimited number of information sources ..., Second, the Internet has no "gatekeepers"--no publishers or editors controlling the distribution of information .... Finally, the users of the Internet are also its producers. But every person who taps into the Internet is his [or her] own journalist. In other words, the Internet has shifted the focus of mass communication to the individual ..." [1]

I. INTRODUCTION

In 1992, the Hard Rock Café Licensing Corporation appealed to the Seventh Circuit to find Concession Services Inc. (CSI), the operator of Chicago-area flea markets, liable for contributory trademark infringement. [2] Private investigators hired by Hard Rock to search for counterfeit merchandise had discovered Mr. Iqbal Parvez selling counterfeit Hard Rock t-shirts from stalls in CSI's Tri-State Swap-O-Rama and Melrose Park Swap-O-Rama. [3] The court applied tort law principles to find liability only in cases where the operator knew or had reason to know that the infringing activity was taking place. [4] Although CSI would have been liable if it had known or should have known that Parvez was selling Hard Rock t-shirts, it had no affirmative duty to ferret out or prevent such illegal activity. [5]

Nine years later, in 2001, Gucci America, Inc., the high-end fashion apparel and accessory house, sued Mindspring Enterprises for contributory trademark infringement and unfair competition, because the web hosting service hosted a website advertising jewelry sold under the Gucci trademark. [6] Mindspring had not responded to Gucci's two emails notifying Mindspring of the infringement. [7] Similarly, in 2008, eBay Inc. was sued for claims that "live bidding" at its "carefully screened" third party auction houses was safe. [8] The plaintiff claimed that eBay's own marketing representations were false, and that vendors employed shill bidders to increase product costs. [9]

Should web hosts like Mindspring and online auction houses like eBay be held to the same standard as CSI, a brick-and-mortar flea market operator? Or does the Internet require special treatment due to its higher value as a vast source of information, communication, and social networking? On one hand, the Internet is a developing resource that the free market could shape without governmental regulation. [10] Additionally, it is likely technologically infeasible for Mindspring or eBay to screen every vendor and product that passes through its virtual universe. [11] On the other hand, consumers deserve protection from false and deceptive marketing practices of those who take advantage of the Internet's lack of accountability. [12]

Congress provided a partial (and vague) answer to this question when it enacted § 230 of the Communications Decency Act (CDA). [13] § 230 provides a safe harbor for Internet service providers (ISPs) from liability for third party actions. [14] The intent of § 230 was to encourage the growth of the Internet [15] and to provide protection for those "Good Samaritans" who take measures to screen or filter indecent or otherwise offensive content. [16] § 230 has been applied to immunize ISPs from an array of civil actions, including false representations, fraud, and unfair business practices. [17] The exact scope of § 230's reach is yet unclear, however, as courts have found that it does not provide blanket immunity for false or deceptive marketing practices. [18]

An investigation into the legislative history of the statute, and the case law that followed its enactment, sheds light on the future of § 230's protection against marketing liabilities. The legislative history and case law suggest litigation strategies that are likely to be effective for plaintiff consumers and defendant website hosts and auction houses. Because recent cases show that courts may shield ISPs and forum websites for some actions but not others

under the CDA, [19] the CDA succeeds to some extent in balancing consumer's and ISP's needs on the Internet. However, Internet commerce needs additional solutions to protect consumers while at the same time fostering the growth of the virtual market. This paper discusses some strategies for balancing consumer and ISP interests, through both governmental and private regulation.

II. THE PROBLEM FOR CONSUMERS

Although the Internet marketplace is convenient, it is fraught with risk for the American consumer. [20] It is open 24 hours per day, 7 days per week, and 365 days of the year, and the consumer is not even required to leave home to take advantage of online wares or services. Amongst a myriad of other tasks, a consumer can buy groceries, [21] airline tickets, [22] or a diamond engagement ring, [23] reserve opera tickets, [24] trade baseball cards, [25] or find a pet to adopt. [26] In the Internet marketplace, price comparisons are a click away, [27] and there are no lines of impatient customers at the cash register.

The price consumers pay for this convenience, however, is steep. [28] Consumers are inundated with emails containing viruses and spam, and easily may be tricked into revealing credit card numbers and other identifying information to dishonest parties. [29] Information released to a reliable site could be discharged inadvertently to non-trusted parties who could use the information for identity theft or to harass or defraud the consumer. [30] Vendors on online auction houses like eBay may misrepresent their wares, sell counterfeit items, or simply not send an item to a consumer after payment. [31] Of reported Internet crimes, online auction fraud accounted for approximately 45% of offenses, by far the most reported crime. [32] Two employees hired by Tiffany to work with eBay over a five month period removed over 19,000 auctions that were selling counterfeit Tiffany merchandise. [33] A random program of Tiffany jewelry purchase through eBay auctions revealed that 73% of the purchased items were counterfeit. [34] Similarly, LVMH Moët Hennessey Louis Vuitton and Christian Dior Couture, two Paris fashion houses, purchased 150,000 Vuitton items and 300,000 Dior items to find that 90% were counterfeit. [35] Accordingly, consumers have reason to be wary in purchasing goods on the Internet, particularly if they plan to invest large amounts of money in high-end products. [36]

The anonymity of the Internet makes it easy, particularly for small companies and individuals, to hide and to avoid responsibility for their illegal actions. [37] Small companies can use false email headers and anonymous remailers to make their steps difficult to trace, and alter computer records to cover up fraud. [38] If caught, these companies may disappear to leave plaintiff consumers with a default judgment that will never be paid, [39] file for bankruptcy, [40] or simply move offshore, outside the jurisdiction of the United States. [41] Once a small company is caught by a consumer or kicked off of a server, it may change its name or re-open on a new server to conduct business almost immediately to deceive a new customer. [42]

Additionally, many consumer contracts with Internet vendors are adhesive in nature [43] and require the consumer to waive their legal rights and remedies, without adequately disclosing that obligation. [44] These contracts may also have choice of law or choice of forum clauses that establish how or where potential disputes will be resolved [45]--usually in a place and manner very convenient and favorable to the seller and inconvenient and unfavorable to the buyer. In addition, the providers of a forum for buyers and sellers, like eBay or Amazon.com, may be held to be immune from liability for crimes against consumers under § 230 of the CDA. [46] This immunity makes it difficult for consumers to obtain a remedy from defendants with deep pockets, or any remedy at all in cases where a vendor cannot be found [47] due to lack of accurate or verifiable record-keeping by the forum. [48] Safe harbors like CDA § 230 must be interpreted in a way that protects consumers by holding parties responsible for their part of harm perpetrated on consumers. Thus, Internet consumers put themselves at great risk to take advantage of the convenience of the Internet, but are afforded relatively little protection from superhighway wrongdoers, with so few options for remedies for Internet misdeeds. [49]

III. THE PROBLEM FOR ISPS AND FORUM WEBSITES

The Internet is a vast and widely-known cyberworld with positive applications for personal and professional networking, information dispersion, and commerce. Many of us cannot even remember what we did when we could not “Google” the answer to a trivia question, map directions to our favorite restaurant, locate the whereabouts of an

old friend, identify new gaming buddies, or determine the next reading assignment for a class. ISPs like America Online (AOL), Verizon, and Comcast provide access to 246,822,936 Internet users in North America alone. [50] These ISPs provide users with search engines to enable them to locate information they seek and forums across which users can chat or trade goods. ISPs are inundated with third party content from these 246 million users in the United States, only a fraction of the estimated 1,581,571,589 users across the world. [51] Online auction houses that provide virtual marketplace forums for buying and selling goods between third parties offer an estimated 1.7 million items at any point in time. [52] With so many users and opportunities for exchange, ISPs and forum hosts afford a bastion of opportunity for free speech and expression.

Given these large numbers, the general growth of the Internet, and the increasing sophistication of cyber-crime technology, it is likely too much to ask of ISPs and forum hosts to screen and filter the entirety of third party content on their sites. [53] EBay already boasts approximately 1000 employees who seek out illegal auctions, but the group is dwarfed by the overwhelming amount of wares that cross the site each day. [54] The problem lies not only in properly allocating resources to police the Internet, [55] but also in identifying and defining what constitutes offensive or illegal conduct. Holding auction forums like eBay responsible for fraudulent content or misrepresentation of vendors may have a chilling effect on constitutionally protected commercial speech. [56] Further, without protection from liability, ISPs and online forums that do take measures to protect users could face the threat of litigation from every direction. [57] Through their "Good Samaritan" actions, they could face legal accountability for satisfying the scienter requirement for criminal statues, and from lawsuits brought both by parties injured by content and parties whose content was deleted. [58]

Thus, § 230 of the CDA protects ISPs and online forums from undeserved liability due to third party actions. The United States District Court for the District of Columbia observed:

> 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 newspapers, 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. [59]

ISPs and online forums, however, should be careful about marketing claims they themselves publish on their sites. [60] They should not be permitted to escape liability for their own controllable and reviewable actions at the expense of such vulnerable consumers.

IV. THE COMMUNICATIONS DECENCY ACT, § 230: LEGISLATIVE HISTORY

As its name suggests, the Communications Decency Act (CDA) originally was not written to address false advertising on the Internet per se. [61] Instead, Congress wrote the CDA as part of the Telecommunications Act of 1996 in an attempt to regulate pornography and other "offensive" material on the Internet. [62] Senator Exon, brandishing his "Blue Book," a notebook of pornographic materials downloaded from the Internet, embarked on a crusade to shelter American children from indecent online material. [63] The CDA criminalized those who made obscene or offensive materials indiscriminately accessible through the Internet to the public. [64] Exon and his committee drafted the CDA expansively, viewing government regulation as the solution to the "red light district" of the Internet, and the Senate overwhelmingly voted its approval. [65]

In the House, however, the CDA did not fare as well. The House viewed the enactment as an unwarranted governmental intrusion on individual and family life, as well as an abridgement of free speech. [66] As an alternative to the CDA, Representatives Cox and Wyden introduced the Internet Freedom and Family Empowerment Act, which rejected government regulation of the Internet and encouraged the more libertarian ideal of individual and market control of Internet content. [67] The House was also aware of a 1995 court decision [68] holding an ISP liable for its editorial role in screening customer content, thus exposing ISPs to responsibility for libel and other torts committed by third parties. Representative Cox and Senator Feingold did not want ISPs to restrict their customers' free speech because they feared liability from that speech. [69] Thus, § 230 provides a safe harbor to protect such "Good Samaritan" efforts of ISPs and forum hosts, [70] and to encourage the growth and development of the Internet. [71] Similarly, this section also protects ISPs from liability for restricting access to particular material or providing the technical means to restrict access to that material. [72] The House voted almost unanimously to pass

the bill, and the CDA in its entirety became law in February, 1996. [73] The portion of CDA § 230 that provides the Good Samaritan safe harbor reads:

> (c) Protection for "Good Samaritan" blocking and screening of offensive material
> (1) Treatment of publisher or speaker
> No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider.
> (2) Civil liability
> No provider or user of an interactive computer service shall be held liable on account of--
> (A) any action voluntarily taken in good faith to restrict access to or availability of material that the provider or user considers to be obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable, whether or not such material is constitutionally protected; or
> (B) any action taken to enable or make available to information content providers or others the technical means to restrict access to material described in paragraph (1). [74]

Additionally, CDA § 230(e) states that the CDA shall not have any effect on criminal laws or intellectual property laws. With regards to state laws, § 230(e)(3) states, "Nothing in this section shall be construed to prevent any State from enforcing any State law that is consistent with this section." Further, CDA § 230(f) defines the terms "information content provider," "interactive computer service," and "access software provider."

Interestingly, the U.S. Supreme Court later overturned most of the CDA as unconstitutionally vague in *Reno v. American Civil Liberties Union*, 521 U.S. 844, 874 (1997), setting aside Senator Exon's rhetoric about innocent children wandering into the Internet red light district. § 230, with its emphasis on free speech and a free market, [75] however, was retained and left undisturbed. [76] Later court decisions have interpreted the provision broadly to immunize ISPs and other service providers from liability for numerous actions of third parties, including torts related to false advertising. [77]

V. THE COMMUNICATIONS DECENCY ACT, § 230: *MAZUR V. EBAY* AND OTHER CASE LAW

The recent case of *Mazur v. eBay, Inc*. [78] provides a comprehensive summary of CDA § 230 judicial interpretation with respect to false advertising claims, as well as a useful context in which to view past case law. Michele Mazur, an eBay user, brought suit against eBay and Hot Jewelry Auctions.com (HJA, an auction house that holds auctions on eBay), alleging violations of California Unfair Competition Law, willful deception and deceit, actual and constructive fraud, unjust enrichment, and negligence. [79] In support of her claims, Mazur contended that "eBay made misrepresentations about Live Auctions in order to intentionally attract and defraud its customers. Specifically, eBay misstated that live auctions were 'safe,' involved 'floor bidders' and were carried out by 'carefully-screened, reputable international auction houses."' [80] Instead, Mazur maintained that the auction house HJA had participated in shill bidding, the prohibited practice of entering fake bids. [81] EBay responded that it was immune from liability under CDA § 230. [82]

In the analysis of eBay's § 230 defense, Judge Patel, writing for the Northern District of California, looked to the text of the statute defining an "interactive computer service" and an "information content provider." [83] Because eBay qualified as an "interactive computer service" and HJA fit the definition of an "information content provider," the court found that eBay could not be held liable for information provided by HJA. [84] This immunity from liability for third party content is the essence of the § 230 safe harbor as described in prior case law. For example, in the case of *Corbis Corp. v. Amazon.com, Inc*., Corbis Corporation alleged that Amazon.com engaged in unfair competition and violated the Washington Consumer Protection Act when it published copyrighted photos on its third party vendor forum called zShops. [85] The court noted that both parties agreed that zShops provided the images that were displayed on its sites, and then pronounced, "[a]lthough Amazon may have encouraged third parties to use the zShops platform and provided tools to assist them, that does not disqualify it from immunity under § 230 because the zShops vendor ultimately decided what information to put on its site." [86]

Similarly, in another recent case, *Gregerson v. Vilana Financial, Inc.*, a defendant alleged a counterclaim of deceptive trade practices against a plaintiff who sought to hold the defendant liable for copyright infringement. [87] The defendant, a corporation offering mortgage, financial, and real estate services, allegedly used the plaintiff's photos in advertisements printed in a telephone book, newspapers, and on its website. [88] The plaintiff, a

photographer, in turn set up a forum on his website for third parties to criticize the defendant. [89] Third party comments ranged from legal analysis to negative comments about the defendant. [90] The court applied CDA § 230 to shield the plaintiff from liability for comments posted on his website by third parties. [91] Thus, the court's finding in the *Mazur v. eBay* case that eBay was not liable for third party content was not surprising, given prior case law like *Gregerson v. Vilana Financial, Inc*. and *Corbis Corp. v. Amazon.com, Inc.*, that interpret CDA § 230 to provide immunity to ISPs and other forums from liability for content that is not their own. [92]

The *Mazur* court also addressed Michele Mazur's contention that eBay knew of HJA's illegal conduct, but failed to prevent it. [93] The opinion made short work of dismissing this argument, stating that whether or not eBay knew of the illegal practices, it was immune under CDA § 230. [94] Judge Patel noted that a prior case with similar facts had found that "[t]his is the classic kind of claim ... found to be preempted by section 230 ... one that seeks to hold eBay liable for its exercise of a publisher's traditional editorial functions." [95] With this finding, the *Mazur* court again followed a CDA § 230 interpretation already established in case law. [96]

The first and most well-known case on the issue of a publisher's editorial function is *Zeran v. America Online, Inc.*. [97] In *Zeran*, the plaintiff's name and phone number had been posted on America Online's (AOL) virtual bulletin board and associated with t-shirts and slogans glorifying the Oklahoma City bombing. [98] The plaintiff, who was not involved in the postings or even an AOL customer, notified AOL, but messages continued to be posted. [99] The plaintiff sued AOL in negligence for allowing the messages to remain or reappear, on the theory that since the plaintiff had notified AOL of the messages, AOL "knew or had reason to know" that the plaintiff could be harmed. [100] The Fourth Circuit, however, bent over backwards to provide AOL with CDA § 230 immunity. First, the court found that Washington State negligent distributor laws were in conflict with the CDA, and thus under the language of the statute, must be preempted by CDA § 230. [101] Second, the court applied the statute retroactively, suggesting that Congress intended the CDA to apply to lawsuits brought before enactment of the CDA, even where the conduct in question occurred prior to enactment of the CDA. [102]

The case of *Universal Communication Systems, Inc. (UCS) v. Lycos, Inc*. [103] also supports the irrelevance of notice to receiving immunity under CDA § 230, but in a context closer to the area of marketing misrepresentations. In that case, a third party posted a number of comments disparaging the "financial condition, business prospects and management integrity" of UCS on a Lycos financially-oriented message board called Raging Bull.com. [104] UCS contended that the postings were "false, misleading and/or incomplete," [105] and that Lycos was aware of the "illegal nature" of the postings. [106] Although UCS argued that Lycos was involved with Raging Bull.com's activities through operation of the website, the court still found that there was no evidence that Lycos was responsible for the creation or the development of the allegedly inaccurate information. [107] Because Lycos merely allowed others to develop and disseminate the material, it was eligible for CDA § 230 immunity from liability. [108] Thus, unlike CSI in the *Hard Rock* case, ISPs and other forums do not incur liability even when they know or have reason to know about offensive content postings and fail to delete them, due to the protection of CDA § 230. [109]

Similarly, Judge Patel in the *Mazur* case found that eBay's online statement claiming that it screened auction houses also was not actionable under CDA § 230. [110] "Screening a potential auction house when deciding whether to include it in Live Auctions is akin to deciding whether to publish and therefore eBay is immune under section 230 for its screening decisions." [111] Although this screening allegation against eBay was analyzed under CDA § 230(c)(1), it might have been more appropriately analyzed under CDA § 230(c)(2). [112] It is unclear whether screening auction houses for quality is a traditional editorial function as described originally in *Zeran*. [113] Further, unlike CDA § 230(c)(1), CDA § 230(c)(2) specifically mentions restricting access to or availability of offensive material as a requirement for obtaining immunity. [114]

While there are fewer false advertising cases analyzing CDA § 230(c)(2), and particularly CDA § 230(c)(2)(B), there is one case that demonstrates how broadly prior courts have interpreted CDA § 230 immunity. In the case of *Zango, Inc. v. Kaspersky Labs, Inc.*, Zango claimed that software anti-virus / anti-malware company Kaspersky improperly identified Zango's wares as malware, and brought an action for tortuous interference with contract and business expectancy, trade libel, and violation of Washington State's Consumer Protection Act. [115] Following the definitions of the statute, the court found that Kaspersky qualified as a "provider" of an "interactive computer service," and an "access software provider" that "provides or enables computer access by multiple users to a computer server." [116] Kaspersky was thus immunized under CDA § 230 for its screening and blocking functions,

not unlike eBay's attempts to screen its auction houses. [117] Thus, broad interpretation of CDA § 230 provisions may have afforded eBay immunity for its screening claim even under more than one provision of the statute.

Despite eBay's CDA § 230 immunity from liability for third party content and screening, its affirmative representations that the auctions were "safe" and involved "floor bidders" were not protected under the statute. [118] In so holding, the court distinguished *Mazur* from three prior cases, *Gentry v. eBay, Inc., [119] Doe v. Sexsearch.com*, [120] and *Prickett v. InfoUSA, Inc.*. [121] In *Gentry*, online buyers claimed that eBay violated California's autographed sports memorabilia statute, failed to provide certificates of authenticity, distributed false certifications, and permitted false representations by its auction houses. [122] The court, however, found that CDA § 230 immunized eBay against the claims, including those involving allegedly false representations by eBay itself. [123] Judge Patel distinguished *Mazur* because eBay's statement of "safety" in that case was "unequivocally stated, of its own volition," [124] while safety claims in *Gentry* were made on the basis of user feedback. [125] Judge Patel additionally observed that cautionary notes [126] in the eBay Live Auction User Agreement did not save it from liability, because they did not negate the fact that eBay vouched for the safety of live auctions. [127]

Next, the *Mazur* opinion distinguished *Sexsearch.com* in addressing eBay's contention that its representations were false only due to third party conduct, which is the type of liability against which CDA § 230 protects. [128] In *SexSearch.com*, the website claimed that its users were all over eighteen years of age, but that claim was merely a recital of its users' assertions. [129] Users knew that there was no age verification procedure, and SexSearch provided an explicit waiver stating that it did not guarantee and did not verify user ages. [130] Judge Patel distinguished *Mazur* because eBay in that case did not present "any evidence regarding safety assurances it received from HJA ... [and t]hough eBay's Live Auctions User Agreement disavows any guarantee that participating auction houses maintain licenses or comply with applicable laws, nothing specifically states that eBay does not guarantee that bidding in Live Auctions is safe." [131] Thus, with no explicit waiver, eBay could not receive immunity under CDA § 230. [132]

Lastly, Judge Patel addressed eBay's assertion that *Prickett* applied to the *Mazur* case. [133] In *Prickett*, the defendant directory listing service received immunity under CDA § 230 although it assured its customers of the quality of its information through a verification process of calling businesses. [134] Judge Patel distinguished *Prickett* because InfoUSA's failure to verify a listing fell within the publisher's editorial function, and thus within CDA § 230's ambit. [135] In contrast, eBay in *Mazur* did not assure customers of accuracy or make promises to remove misbehaving auctioneers, but instead asserted the safety of Live Auctions. [136] The opinion states, "eBay's statement regarding safety affects and creates an expectation regarding the procedures and manner in which the auction is conducted and consequently goes beyond traditional editorial discretion." [137] Arguably, Judge Patel walks a thin line on this point, as safety seems to have a special and likely exceptional meaning to her. [138] The distinction between *Mazur* and *Prickett*, however, may suggest a trend for future cases of holding ISPs and online forums responsible for their claims of user security and protections. [139]

Interestingly, the *Mazur* opinion did not mention *Curran v. Amazon.com, Inc*. [140] or *Federal Trade Commission v. Accusearch, Inc.*, [141] both of which have comparable fact patterns to *Mazur*. *Accusearch* involved the sale of telephone records procured from third party vendors through the illicit means of pretexting. [142] Accusearch allegedly knew that that the information it resold was confidential and that it was obtained underhandedly. [143] The Wyoming District court found that "by soliciting requests for ... phone records and purchasing them for resale, Defendants 'participat[ed] in the creation or development of [the] information, and thus [do] not qualify for § 230 Immunity."' [144] In both *Mazur* and *Accusearch*, the defendant did not receive immunity because its actions extended beyond traditional editorial functions. [145] Both cases, however, also involved an underlying deception of consumers and misrepresentations of information presented. [146]

In the similar case of *Curran v. Amazon.com*, the defendant CafePress, through partnership with a third party, sold t-shirts with three designs featuring the plaintiff's likeness without the plaintiff's consent and without providing the plaintiff with monetary compensation. [147] According to the plaintiff, "CafePress sets the base price for the t-shirt, determines the type of product its joint venture partner may sell, manufactures and prints the t-shirts, and earns money from each t-shirt sold on its website." [148] Thus, the plaintiff identified CafePress as an "information content provider," undeserving of CDA § 230 immunity. Although CafePress responded that it was instead an "interactive computer service" qualifying for immunity, the court held that it did not provide enough evidence for a

motion to dismiss and postponed the issue until after discovery. [149] The CafePress opinion provides another example of a defendant being denied CDA § 230 immunity due to underlying third party illegal actions. [150] It remains unclear whether CafePress' partner or CafePress itself took part in the illegality, [151] but it nonetheless provides another apt analogy for the eBay case, wherein an ISP reached beyond its traditional editorial functions to participate in the development of content on the Internet. [152] These cases may reflect a trend to hold ISPs and other online forums responsible for third party consumer deception or fraud and illegal behavior.

VI. CDA § 230 Litigation Strategies for Plaintiffs and Defendants

Different courts' interpretations of the text of CDA § 230 suggest litigation strategies for plaintiffs and defendants when CDA § 230 immunity is asserted. Obviously, a party's ability to follow these strategies ethically will depend on the facts of the particular case, but these strategies may assist a party in representing facts in a particular light, thus creating a coherent story of the case favorable to its goals. For example, plaintiffs should assert that the defendant is an "information content provider" and not an Internet service provider. A plaintiff may claim that the defendant's activities extended beyond traditional editorial functions into creation and development of content. It is also helpful if the facts allow a plaintiff to assert that third party activity in which the defendant may or may not be involved is illegal or underhanded in some way.

These strategies have been successful in a number of cases. One example is the *Gregerson* case, in which the plaintiff photographer was not immunized under CDA § 230 for his own comments criticizing the counterclaiming defendant Vilana Financial. [153] Another example is a case involving fraud and negligent misrepresentation claims against an online dating service, wherein it was alleged that the service created false user profiles in order to deceive new clients into participating and to stop current users from discontinuing the service. [154] The operator of the dating service was accused of creating the content in the profiles in question, and not merely posting content created by a third party, thus rendering him ineligible for CDA § 230 immunity. [155] A final example in this category of plaintiff strategies is the *Accusearch* case, in which the FTC asserted that the process of procuring telephone record information (pretexting) that Accusearch resold was illegal. [156] Accusearch, which likely knew of the underlying illegality, was then denied immunity under CDA § 230. [157]

In contrast to a plaintiff's litigation strategy when CDA § 230 is asserted, defendants raising the defense should make it clear that the material about which the plaintiff complains was provided by a third party. Defendants should also beware of their involvement with third party content development and pay attention to content legality. These procedures would show that the defendant is an Internet service provider and not an "information content provider," and does not extend its activities beyond traditional editorial functions. In this way a defendant could be eligible for CDA § 230 immunity.

The *Gregerson* and *Mazur* cases demonstrate the efficacy of this strategy. [158] In *Gregerson*, the plaintiff photographer was immunized from liability for third party comments posted on his website, but not for his own negative statements about the defendants. [159] If he had not made his own comments but merely allowed third parties to complain, he would have been eligible for immunity under CDA § 230. [160] In *Mazur*, eBay was similarly immunized only for content attributable to third parties. [161] EBay was not protected for its own claims, and other activities that extended beyond traditional editorial functions. [162] When a defendant's own conduct makes it an "information content provider" instead of an Internet service provider, it loses immunity under CDA § 230. [163]

In addition, plaintiffs should frame their claims so that they fall under intellectual property (IP) law, or even better, federal IP law. IP law claims are exempted from the CDA § 230 safe harbor. [164] Alternatively, a plaintiff could assert that its state law claims are IP claims. [165] This strategy for framing claims so that they fall outside the ambit of CDA § 230 has been successful in many cases. One such prominent false advertising-related case is *Gucci v. Hall*, described above. [166] In *Gucci*, the plaintiff claimed violations of the Lanham Act, including false advertising, which as a federal IP law is exempt from CDA § 230 immunity. [167] Further, the court ruled, albeit without much analysis, that the plaintiff's trademark infringement and unfair competition claims under New York state law were considered intellectual property claims. [168] Thus, the defendants were not eligible for CDA § 230 protection, and the court denied the defendants' motion to dismiss. [169]

Defendants, in turn, should take pains to remind the court that CDA § 230 immunity applies to state law claims, including IP-related claims. Because CDA § 230 does not apply to IP claims, plaintiffs ineligible for federal intellectual property protections may attempt to draft claims artfully as state IP claims (see above). In response, defendants must contend that multiple cases suggest otherwise. *Perfect 10, Inc. v. CCBill LLC* [170] provides an example of a case where a defendant was able to claim immunity under § 230 from IP-related state law claims. In *Perfect 10*, the plaintiff publisher claimed that the web-host defendants violated state unfair competition, false advertising, and right of publicity laws by providing services to clients that posted images stolen from the plaintiff's publications. [171] The court noted that state laws have not established definitions of "intellectual property," and however defined, the laws are not uniform. [172] Permitting any one state's laws to reach across the country via the Internet would frustrate Congress' expressed goal of allowing the growth of the Internet "unfettered by ... state regulation." [173] Thus the court interpreted the term "intellectual property" in § 230 to mean "federal intellectual property," bringing the plaintiff's state law claims within the reach of § 230 to immunize the defendant. [174]

Additionally, plaintiffs and defendants obviously will advance different policy arguments to support their contentions. Plaintiffs will emphasize the need for consumer protection on the Internet, and the current lack of effective remedies available for plaintiffs. [175] ISPs and online forums make money from these consumers, and should take responsibility for material they create, develop, or even disseminate. [176] After all, the goal of Congress in enacting the CDA was to shield users from offensive material. [177] Defendants, on the other hand, must stress that the goal of Congress was to promote the growth of the Internet as a resource, shielding it from federal and state laws, and to promote free speech. [178] Further, it would be logistically impossible for ISPs to police all content in their respective universes, due to the large volume of information that crosses the Internet. [179]

These strategies all take advantage of gaps left by Congress in the CDA, which courts have yet to interpret. Once there is more certainty in this area, i.e., when Congress clarifies the statute, or a high court interprets the text for lower courts to follow, parties may be forced to rethink their strategies.

VII. Balancing Consumer Interests While Protecting Internet Business Development

The law has yet to catch up with the quickly evolving world of Internet commerce. The challenge of developing rules to govern Internet commerce is to satisfy the needs of both consumers and Internet businesses. The *Mazur* case arguably provides a way for plaintiff consumers to dodge the CDA § 230 defense in false advertising cases. [180] Now, plaintiffs know that they should not merely assert a prima facie case against an ISP or online forum for third party misbehavior. [181] To insure that a false marketing claim is outside CDA § 230's ambit, a plaintiff should search a website for a representation (actual or implied) that a tort will not occur, and base claims on the tort's occurrence. [182] This bypass around CDA § 230 occurred in *Mazur* in relation to eBay's "safety" assurances. [183]

Thus, it seems that *Mazur* reasonably balances consumer and Internet business interests. [184] EBay was not held liable for third party actions (i.e., those of HJA), [185] because it would be unfair to expect that eBay could police the millions of items in its auctions satisfactorily. [186] It was also reasonable to resist basing liability on notice of third party bad conduct, as that would likely open up eBay to excessive and undeserved liability, and to protect eBay's traditional editorial functions, because eBay should be encouraged to screen or filter to the best of its abilities. [187] EBay should incur liability, however, for how it markets its business through its own representations. EBay should not be permitted to assert freely a claim that it does not support, in order to entice customers to behave in a certain way that provides economic benefit for eBay. [188] In short, although CDA § 230 has its place in protecting ISPs and online forums from liability for third party misdeeds and its own attempts at screening and filtering, it should not "provide a free pass for commercial misrepresentation." [189]

A federal law that may limit this free pass is the Federal Trade Commission Act (FTCA), enacted in 1914 but updated in 2000 by the FTC working paper "Dot Com Disclosures" to apply to online marketing practices. [190] The FTC noted that its "role in protecting consumers from unfair or deceptive acts or practices encompasses advertising, marketing and sales online." [191] The FTCA requires that advertising must be truthful and not misleading, advertising claims must be substantiated, and advertising must not be unfair. [192] An advertiser must disclose material information, [193] including material connections between an endorser and the product. [194] The

FTC judges the deceptiveness of an advertisement online as it does offline: on the basis of its effect on consumers, not on the intent of the advertiser. [195] Thus, a female plaintiff who purchased a hair product promoted in a chatroom by a male product representative posing as a female may face obstacles in demonstrating that the particular online practice was deceptive. For example, is misrepresenting one's gender online deceptive, or is it considered "acceptable fiction"? [196] And was the plaintiff made aware of the male's connection to the product? [197] Although proving facts and demonstrating consumer perceptions may provide loopholes in the FTCA for defendants, defendants facing claims arising under the FTCA are likely exempt from CDA § 230 immunity. [198]

Accordingly, if Congress intends to provide complete or partial immunity for deceptive advertising on the Internet, for websites or third parties, it should write clear law for that purpose, as it did to create a safe harbor against liability for copyright infringement in the Digital Millennium Copyright Act and (originally) obscenity in the CDA. [199] Congress would need to set standards for determining whether an ISP or website has gone beyond its "traditional editorial function" in order to deceive customers for profit. [200] Additionally, Congress would need to determine the extent to which ISPs and websites are responsible for third party behavior in relation to marketing representations on the website. [201] Arguably, commercial speech is not entitled to the same level of protection as traditional CDA § 230 speech (i.e., critical or potentially offensive speech) and may therefore present a better candidate for governmental regulation. [202] Congress is likely to encounter fewer obstacles, particularly first amendment obstacles, in protecting consumers from false or fraudulent marketing representations on the Internet than in attempting to regulate critical speech.

It would be unwise, however, for the government, particularly Congress, to participate in heavy-handed regulation of the Internet. [203] The vastness of the Internet, and the anonymity it fosters, pose special problems for satisfying needs of both consumers and businesses, distinct from brick-and-mortar marketing concerns. [204] Thus the Internet is an entity that may be better handled by a specialized agency with technical and trade expertise, or better, by the free market. [205] The Internet has spawned novel marketing strategies for businesses, including the guerilla tactic of ads popping onto the screen of unsuspecting Internet users, paying search engines for placement near the top of search results, and using competitor names as metatags. Laws made today to combat these problems may prove ineffective tomorrow as marketers use technology to work around existing legal structures to change consumer behavior. Policing the Internet from the outside, like eBay policing all of its auction houses and items, is impractical and unworkable. [206] Cooperation from Internet businesses is imperative.

One cooperation effort comprising nineteen of the largest Internet companies involves an e-commerce initiative called the Global Business Dialogue on E-Commerce (GBDe). [207] GBDe was formed in 1999 to "assist the development of a global policy framework for the emerging online economy." [208] The group promotes a private sector/government dialogue as part of its efforts, [209] which include development of consumer protection and consumer-business alternative dispute resolution mechanisms. [210] GBDe states that the "mechanisms will be designed to permit consumers ... to enjoy basic protections against false and misleading advertising and marketing practices, and to have access to private redress for violations of those protections." [211] The group also considers jurisdictional issues so that consumers are protected across borders. [212]

A similar group, called the Software and Information Industry Association (SIIA), is a software trade group that polices auction house offerings of pirated software, filing suits against the worst offenders through its Auction Litigation Program. [213] The group's efforts have proven effective at reducing the number of illegal software auctions, as there has been a 20-50% decrease in Symantec and McAfee pirated software auctions on eBay alone. [214] SIIA focuses on copyright infringement, but could be applied easily in trademark and other deceptive advertising contexts. [215]

While the goals of these groups are admirable, significant concerns remain. One wonders where the consumer fits into such groups of monster companies like AOL and IBM, and how GBDe and SIIA go about finding a representative consumer perspective. [216] Self-regulation may not have its desired effect of increasing consumer confidence. [217] It may also be difficult for smaller companies to communicate their concerns. Additionally, it may be that traditional free market, laissez-faire solutions fail on the Internet, since businesses have an increased ability to lay low for a critical time and then crop up under a different name. [218] The temptation to deceive is high in such a vast and anonymous universe. On the Internet, it remains more difficult for businesses to gain reputations (positive or negative), and also for consumers to learn which businesses to avo It is also more difficult for such

dispersed consumers to communicate with each other to organize against businesses with deceptive marketing practices. Geography and jurisdictional issues also pose challenges. [219] Thus for self-regulation to succeed, it is important for Internet businesses and such groups as GBDe and SIIA to communicate with Internet consumers to work toward solutions satisfactory for both parties.

For example, if Internet businesses are afforded protection from liability, like under CDA § 230, they should be willing to provide adequate consideration for it. [220] This may include, for example, requiring that Internet businesses keep accurate records of all user identities with verifiable information, [221] which may help a consumer locate a corrupt auction house. Internet auction forums may offer reasonable prices on consumer insurance to the value of the transaction. [222] User agreements to use online services should be sufficient to explain to the consumer the practices and responsibilities of the business. [223] Self-regulation could include fines for Internet businesses that do not cooperate with rules, and punitive damages could be imposed in legal actions [224] in which defendant Internet businesses intentionally or recklessly indulge in deceptive marketing techniques. Some of these options are already employed by Internet businesses, [225] and courts look upon the exercise of these options favorably when deciding the fate of a defendant, [226] for example granting immunity under CDA § 230. Working together, consumers and Internet marketers can create a reasonable framework to promote fair advertising and business dealings, [227] and at the same time allow the Internet to develop to its full potential. [228]

VIII. CONCLUSION

Internet marketing practices pose a unique challenge to the U.S. government, consumers, and Internet businesses. The Internet is expanding and developing quickly, and deception is easy to achieve given the anonymity allowed by the medium. Some ISPs and online forums have received immunity under CDA § 230 against claims of deceptive marketing practices, but it is difficult to know whether Congress intended the statute to be applied in such a way. CDA § 230 was enacted to promote the growth of the Internet and to provide protection for parties who attempt to screen or filter indecent or otherwise offensive content. While deceptive marketing practices were not a focus of discussion in Congress, there was much support for free market ideals of competition providing its own regulation. Thus, to the extent that CDA § 230 allows some Internet businesses to compete, without undue burden, false advertising could indeed fall under its umbrella.

Recent cases have demonstrated the principle that CDA § 230 provides limited protection for deceptive business practices. In the case of *Mazur v. eBay*, eBay did not incur liability for the third party practices of its auction house, but it did incur liability for its own marketing representations. This result is likely appropriate because eBay would not be able to function if it had to screen every auction house and every item on its virtual floors, due to the enormity of such a task. But, eBay should not be allowed to attract customers based on false statements offered under its control. Cases like *Mazur* have demonstrated for plaintiffs and defendants strategies for arguing in favor of or against CDA § 230 immunity. Parties will likely follow these strategies for the near future, until new laws are enacted or a coherent self-regulation scheme is implemented.

While the government may supply a loose framework of laws to govern deceptive marketing practices on the Internet, through Congress or through an agency, it is likely best left to the Internet community of businesses (large and small) and consumers working together to make and enforce marketing regulations. They understand best the technology, the strategies, and the challenges that they face. Some have already implemented solutions that are looked upon favorably by the courts. Internet commerce has reached its adolescence, but once it works through these growing pains, it will emerge stronger, safer, and more transparent.

APPENDIX: 47 U.S.C. § 230

(a) Findings

The Congress finds the following:

(1) The rapidly developing array of Internet and other interactive computer services available to individual Americans represent an extraordinary advance in the availability of educational and informational resources to our citizens.

(2) These services offer users a great degree of control over the information that they receive, as well as

the potential for even greater control in the future as technology develops.

(3) The Internet and other interactive computer services offer a forum for a true diversity of political discourse, unique opportunities for cultural development, and myriad avenues for intellectual activity.

(4) The Internet and other interactive computer services have flourished, to the benefit of all Americans, with a minimum of government regulation.

(5) Increasingly Americans are relying on interactive media for a variety of political, educational, cultural, and entertainment services.

(b) Policy

It is the policy of the United States--

(1) to promote the continued development of the Internet and other interactive computer services and other interactive media;

(2) to preserve the vibrant and competitive free market that presently exists for the Internet and other interactive computer services, unfettered by Federal or State regulation;

(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;

(4) to remove disincentives for the development and utilization of blocking and filtering technologies that empower parents to restrict their children's access to objectionable or inappropriate online material; and

(5) to ensure vigorous enforcement of Federal criminal laws to deter and punish trafficking in obscenity, stalking, and harassment by means of computer.

(c) Protection for "good Samaritan" blocking and screening of offensive material

(1) Treatment of publisher or speaker

No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider.

(2) Civil liability

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

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

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

(d) Obligations of interactive computer service

A provider of interactive computer service shall, at the time of entering an agreement with a customer for the provision of interactive computer service and in a manner deemed appropriate by the provider, notify such customer that parental control protections (such as computer hardware, software, or filtering services) are commercially available that may assist the customer in limiting access to material that is harmful to minors. Such notice shall identify, or provide the customer with access to information identifying, current providers of such protections.

(e) Effect on other laws

(1) No effect on criminal law

Nothing in this section shall be construed to impair the enforcement of section 223 or 231 of this title, chapter 71 (relating to obscenity) or 110 (relating to sexual exploitation of children) of Title 18, or any other Federal criminal statute.

(2) No effect on intellectual property law

Nothing in this section shall be construed to limit or expand any law pertaining to intellectual property.

(3) State law

Nothing in this section shall be construed to prevent any State from enforcing any State law that is consistent with this section. No cause of action may be brought and no liability may be imposed under any State or local law that is inconsistent with this section.

(4) No effect on Communications Privacy law

Nothing in this section shall be construed to limit the application of the Electronic Communications Privacy Act of 1986 or any of the amendments made by such Act, or any similar State law.

(f) Definitions

As used in this section:

(1) Internet

The term "Internet" means the international computer network of both Federal and non-Federal interoperable packet switched data networks.

(2) Interactive computer service

The term "interactive computer service" means any information service, system, or access software provider that provides or enables computer access by multiple users to a computer server, including specifically a service or system that provides access to the Internet and such systems operated or services offered by libraries or educational institutions.

(3) Information content provider

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.

(4) Access software provider

The term "access software provider" means a provider of software (including client or server software), or enabling tools that do any one or more of the following:

(A) filter, screen, allow, or disallow content;

(B) pick, choose, analyze, or digest content; or

(C) transmit, receive, display, forward, cache, search, subset, organize, reorganize, or translate content.

[1]. Blumenthal v. Drudge, 992 F. Supp. 44, 48 n. 7 (D.D.C. 1998).

[2]. Hard Rock Café Licensing Corp. v. Concession Services Inc., 955 F.2d 1143, 1145 (7th Cir. 1992).

[3]. *Id.*

[4]. *Id.* at 1149.

[5]. *Id.*

[6]. Gucci America, Inc. v. Hall & Assoc., 135 F. Supp. 2d 409, 410-11 (S.D.N.Y. 2001).

[7]. *Id.* at 411.

[8]. Mazur v. eBay Inc., No. C 07-03967, 2008 WL 618988, at *9-*11 (N.D. Cal. 2008).

[9]. *Id.* at *1-*2.

[10]. *See* Vikas Arora. *The Communications Decency Act: Congressional Repudiation of the "Right Stuff."* 34 HARV J. ON LEGIS. 473, 488 (1997).

[11]. Jonathan Band, *The Superhighway to Jericho: Good Samaritan Provisions*, Journal of Internet Law, p. 2, (August 1999), http:// www.policybandwidth.com/doc/JBand-GoodSamaritanProvisions.pdf

[12]. *See* Michael L. Rustad, *Punitive Damages in Cyberspace: Where in the World is the Consumer?*, 7 CHAP. L. REV. 39, 92 (2004).

[13]. *See* 47 U.S.C. § 230.

[14]. *See* 47 U.S.C. § 230(c)(1).

[15]. *See* 47 U.S.C. § 230(b)(1)-(2).

[16]. *See* 47 U.S.C. § 230(b)(3)-(5), (c).

[17]. *See, e.g.*, Perfect 10, Inc. v. CCBill LLC, 488 F.3d 1102 (9th Cir. 2007) (unfair competition, false advertising); Anthony v. Yahoo! Inc., 421 F.Supp.2d 1257 (N.D.Cal. 2006) (fraud, negligent misrepresentation); Zeran v. America Online, Inc., 129 F.3d 327 (4th Cir. 1997) (negligence, fraud).

[18]. *See Mazur*, 2008 WL 618988, at *11.

[19]. *See Id.*

[20]. *See* Michael L. Rustad, *Punitive Damages in Cyberspace: Where in the World is the Consumer?*, 7 Chap. L. Rev. 39, 39-40 (2004).

[21]. *See, e.g.*, Peapod Online Grocery Shopping and Delivery Service, http://www.peapod.com.

[22]. Orbitz--Official Site, http://www.orbitz.com.

[23]. Diamond Ring at Zales, http://www.zales.com/category/index.jsp?categoryId=2109180&cp=2071133&clickid=hmp_weddingdrop_1.

[24]. Boston Opera House Tickets, http://www.tickco.com/venue_ schedules/boston_opera_house.htm.

[25]. Baseball Card Trading, http://www.sportscardfun.com/default.aspx.

[26]. Petfinder, http://www.petfinder.com.

[27]. *See, e.g.*, http://www.pricegrabber.com.

[28]. *See* Rustad, *supra* note 20, at 39-40.

[29]. *See Id.*

[30]. *Id.* (Eli Lilly and Co. accidentally released information from medical patients who had registered at its website to receive emails concerning health-related matters. Although Eli Lilly settled with states, individual patients did not receive damages for the compromise in privacy.)

[31]. *See* Emily Favre, *Online Auction Houses: How Trademark Owners Protect Brand Integrity Against Counterfeiting*, 15 J. L. & POL'Y 165, 166-68 (2007).

[32]. Internet Crime Complaint Center's statistics, http://www.consumerfraudreporting.org/internet_scam_statistics.htm.

[33]. Favre, *supra* note 31, at 192.

[34]. *Id.*

[35]. *Id.* at 194-95.

[36]. *See Id.* at 195-96.

[37]. Rustad, *supra* note 20, at 67-69.

[38]. *Id.* at 66.

[39]. Doe v. GTE Corp., 347 F.3d 655, 656 (7th Cir. 2003) (remarking that online pornographer defaulted when sued by male college athletes for secret filming and online sale of videos).

[40]. Caton v. Trudeau, 157 F.3d 1026, 1028 (5th Cir. 1998) (Internet defendant filed for bankruptcy after libel judgment was entered).

[41]. Kremen v. Cohen, 337 F.3d 1024, 1027 (9th Cir. 2003) (reporting that defendant moved assets to an off-shore haven and defaulted on the judgment).

[42]. Rustad, *supra* note 20, at 67-68.

[43]. *Id.* at 85.

[44]. *Id.* at 87-88.

[45]. *Id.* at 85.

[46]. *See* Lateef Mtima, *Doing Business on the Internet: Avoiding Intellectual Property, Information Dissemination, and Consumer Protection "E-Commerce Liability"*, SN051 ALI-ABA 157, 180 (OCTOBER 18-19, 2007).

[47]. Rustad, *supra* note 20, at 81-84.

[48]. Mary Kay Finn, Karen Lahey, and David Redle, *Policies Underlying congressional Approval of Criminal and Civil Immunity For Interactive Computer Service Providers Under Provisions of the Communications Decency Act of 1996-- Should E-Buyers Beware?*, 31 U. Tol. L. Rev. 347, 372 (2000).

[49]. *See* Rustad, *supra* note 20.

[50]. Internet World Stats, http://www.Internetworldstats.com/stats.htm (last visited March 19, 2009).

[51]. *Id.*

[52]. Finn *et al.*, *supra* note 48, at 351.

[53]. *See* Band, *supra* note 11, at 2.

[54]. Favre, *supra* note 31, at 172.

[55]. *See Id.*

[56]. *See, e.g.*, *Gucci*, 135 F. Supp. 2d at 421 ("Section 230 reflects a 'policy choice' ... to immunize ISPs from defamation and other 'tort-based lawsuits,' driven in part, by free speech concerns.")

[57]. Band, *supra* note 11, at 3.

[58]. *Id.*

[59]. Blumenthal v. Drudge, 992 F. Supp. 44, 49 (D.D.C. 1998).

[60]. *See Mazur*, 2008 WL 618988 at *10.

[61]. *See* 47 U.S.C. § 230(a)-(b).

[62]. Robert Cannon, *The Legislative History of Senator Exon's Communications Decency Act: Regulating Barbarians on the Information Superhighway*, 49 Fed. Comm. L.J. 51, 53 (1996).

[63]. *Id.* at 64; 141 Cong. Rec. S8089 (daily ed. June 9, 1995)

[64]. *Id.* at 57-58.

[65]. *Id.* at 53, 71-72.

[66]. 141 Cong. Rec. H8470 (1995) (statement of Rep. Wyden) ("[The other body seeks] to put in place the Government rather than the private sector about this task of trying to define indecent communications ... [t]he fact of the matter is that the Internet operates worldwide, and not even a Federal Internet censorship army would give our Government the power to keep offensive material out of the hands of children ..."; *See also* 141 Cong. Rec. S5548 (daily ed. Apr. 7, 1995) (statement of Sen. Leahy) ("I introduce a bill calling for a study ... on how we can empower parents and users of interactive telecommunications systems .... We must find ways to do this that do not invite invasions of privacy, lead to censorship of private online communications, and undercut important constitutional protections."

[67]. *Id.*; *See also* 141 Cong. Rec. S5548 (daily ed. Apr. 7, 1995) (statement of Sen. Leahy) ("Instead of rushing to regulate the content of information services, we should encourage the development of technology that gives ... consumers the ability to control the information that can be accessed over a modem.")

[68]. Stratton Oakmont, Inc. v. Prodigy Services Co., 1995 WL 323710 (N.Y. Sup. 1995).

[69]. 141 Cong. Rec. H8469-70 (1995). (statement of Rep. Cox) ("Ironically, the existing legal system provides a massive disincentive for the people who might best help control the Internet to do so."); *See also* 141 Cong. Rec. S8310, S8336 (1995) (statement of Sen. Feingold) ("the opportunity exists to solve at least part of the problem through the marketplace today, not through governmental prohibitions ... None of the technical safeguards available, such as blocking software and provider screening, are perfect, but the nice thing is they do not violate the first amendment."

[70]. 47 U.S.C. § 230(c).

[71]. *See* 47 U.S.C. § 230(b)(1).

[72]. 47 U.S.C. § 230(c)(2).

[73]. Finn *et. al.*, *supra* note 48, at 365.

[74]. 47 U.S.C. § 230(c).

[75]. *See* 47 U.S.C. § 230(b)(2).

[76]. *See Reno*, 521 U.S. at 874.

[77]. *See, e.g.* Batzel v. Smith, 333 F.3d 1018 (9th Cir. 2003) (interpreting § 230 broadly to provide immunity); Gentry v. EBay Inc., 121 Cal. Rptr. 2d 703 (Cal. App. 2002) (CDA § 230 immunity from false advertising claim).

[78]. No. C 07-03967, 2008 WL 618988 (N.D. Cal. 2008).

[79]. *Id.* at *8 (amongst other claims).

[80]. *Id.* at *8.

[81]. *Id.* at *1.

[82]. *Id.* at *8.

[83]. *Id.* at *9; 47 U.S.C. § 230 (f)(2),(3).

[84]. *Id.* at *9.

[85]. 351 F.Supp.2d 1090, 1093-94 (W.D.Wash. 2004).

[86]. *Id.* at 1118.

[87]. Gregerson v. Vilana Financial, Inc., No. 06-1164, 2008 WL 451060, at *1 (D.Minn. 2008).

[88]. *Id.* at *1-*2.

[89]. *Id.* at *4.

[90]. *Id.* (Comments include allegations that defendant "was affiliated with the Russian mafia, that his secretary was his girlfriend and a prostitute, and that [he] is a thief.")

[91]. *Id.* at *9 (As we will see later, the plaintiff was liable for only for his own comments on his website.).

[92]. *See Gregerson*, 2008 WL 451060; *Mazur*, 2008 WL 618988; *Corbis Corp.*, 351 F.Supp.2d at 1090.

[93]. *Mazur*, 2008 WL 618988, at *9.

[94]. *Id.*

[95]. *Id.* (quoting Barrett v. Rosenthal, 146 P.3d 510 (Cal. 2006)) (traditional editorial functions include deciding whether to publish, withdraw, postpone, or alter content.).

[96]. *Id.*

[97]. 129 F.3d 327 (4th Cir. 1997).

[98]. *Id.* at 329.

[99]. *Id.*

[100]. *Id.* at 331-33.

[101]. *Id.* at 334; *see* CDA § 230(e)(3).

[102]. *Id.* at 334-35.

[103]. 478 F.3d 413 (1st Cir. 2007).

[104]. *Id.* at 416.

[105]. *Id.*

[106]. *Id.* at 420.

[107]. *Id.* at 420-21.

[108]. *Id.*

[109]. *See Id.; Mazur*, 2008 WL 618988; *Zeran*, 129 F.3d at 327.

[110]. *Mazur*, 2008 WL 618988, at *9.

[111]. *Id.* (that eBay maintained that it "carefully" screened for "reputable" auction houses did not change its eligibility for immunity, as the modifiers "carefully" and "reputable" both indicated an opinion and thus were not actionable.)

[112]. Eric Goldman, Technology and Marketing Law Blog, "eBay Denied 230 Defense for Its Marketing Representations--Mazur v. eBay" http:// blog.ericgoldman.org/archives/2008/03/ebay_denied_230.htm (March 13, 2008).

[113]. *Id.*

[114]. CDA § 230(c)(1)-(2).

[115]. No. C07-0807-JCC, 2007 WL 5189857 at *1 (W.D. Wash. 2007).

[116]. *Id.* at *3-4.

[117]. *Id.* at *4.

[118]. *Mazur*, 2008 WL 618988, at *10-12.

[119]. Gentry v. eBay, Inc., 121 Cal. Rptr. 2d 703 (Cal. App. 2002).

[120]. Doe v. Sexsearch.com, 502 F. Supp. 2d 719 (N.D. Ohio 2007).

[121]. Prickett v. InfoUSA, Inc., No. 4:05-CV-10, 2006 WL 887431 (E.D. Tex. 2006).

[122]. *Gentry*, 121 Cal. Rptr. 2d at 706.

[123]. *Id.* at 716-17.

[124]. *Mazur*, 2008 WL 618988, at *10

[125]. *Id.*, *Gentry*, 121 Cal. Rptr. 2d at 717-18.

[126]. *Mazur*, 2008 WL 618988, at *10 ("eBay argues that it makes clear in its Live Auction User Agreement that it: 1) only provides a venue; 2) is not involved in the actual transaction between buyer and seller; and 3) does not guarantee any of the goods offered in any auction").

[127]. *Id.*

[128]. *Id.* at *11.

[129]. *Sexsearch.com*, 502 F. Supp. 2d at 729.

[130]. *Id.* at 729-30.

[131]. *Mazur*, 2008 WL 618988 at *11.

[132]. *Id.*

[133]. *Id.*

[134]. *Prickett*, 2006 WL 887431, at *3, *5

[135]. *Mazur*, 2008 WL 618988, at *12.

[136]. *Id.*

[137]. *Id.*

[138]. Goldman, *supra* note 112.

[139]. *See Mazur*, 2008 WL 618988; *Prickett*, 2006 WL 887431.

[140]. No. 2:07-0354, 2008 WL 472433 (S.D.W. Va. 2008).

[141]. No. 06-CV-105-D, 2007 WL 4356786 (D. Wyo. 2007).

[142]. *Id.*

[143]. *Id.* at *6-*7.

[144]. *Id.* at *6 (quoting *Ben Ezra, Weinstein, and Co. v. America Online, Inc.*, 206 F.3d 980, 985 n. 4 (10th Cir. 2000)).

[145]. *Id.*; *Mazur*, 2008 WL 618988, at *12.

[146]. *See Id.*

[147]. *Curran*, 2008 WL 472433 at *1, *3, *11 (the plaintiff alleged an invasion of his right to privacy and right to publicity and the defendant argued that CDA § 230 immunity applied to both claims).

[148]. *Id.* at *2.

[149]. *Id.* at *12-*14.

[150]. *See Id.*

[151]. *See Id.*

[152]. *See Id.*; *Mazur*, 2008 WL 618988.

[153]. *See Gregerson*, 2008 WL 451060 (D. Minn. 2008).

[154]. *Anthony v. Yahoo! Inc.*, 421 F.Supp.2d 1257 (N.D.Cal. 2006).

[155]. *Id.* at 1262-63.

[156]. *Accusearch*, 2007 WL 4356786, at *6-*7.

[157]. *Id.* at *5-*6.

[158]. *See Gregerson*, 2008 WL 451060; *Mazur*, 2008 WL 618988.

[159]. *Gregerson*, 2008 WL 451060, at *9.

[160]. *See Id.*

[161]. *Mazur*, 2008 WL 618988, at *9-*10.

[162]. *Id.* at *12.

[163]. *See Gregerson*, 2008 WL 451060; *Mazur*, 2008 WL 618988.

[164]. 47 U.S.C. § 230(e)(2).

[165]. 47 U.S.C. § 230(e)(2)-(3).

[166]. *Gucci*, 135 F. Supp. 2d 409.

[167]. *Id.* at 421.

[168]. *Id.* at 415.

[169]. *Id.* at 421-22.

[170]. 488 F.3d 1102 (9th Cir. 2007).

[171]. *Id.* at 1108.

[172]. *Id.* at 1118-19.

[173]. *Id.*; 47 U.S.C. § 230(b)(2).

[174]. *Id.* at 1119 (Even if the plaintiff submits an intellectual property claim under the Lanham Act, the defendant may assert the "innocent infringer" defense under 15 U.S.C. § 1114(2) (§ 32(2) of the Lanham Act). An infringer is "innocent" unless it acted either 1) with knowledge of the infringement or 2) with reckless disregard as to infringement. *See Gucci*, 135 F. Supp. 2d at 419.)

[175]. *See, e.g.*, Rustad, *supra* note 12.

[176]. *See Id.*

[177]. *See, e.g.*, Finn *et. al., supra* note 48, at 358.

[178]. 47 U.S.C. § 230 (b)(1)-(2).

[179]. *See, e.g.*, Band, *supra* note 11.

[180]. Goldman, *supra* note 112; s*ee Mazur*, 2008 WL 618988.

[181]. *See Id.*

[182]. *See Id.*; *Mazur*, 2008 WL 618988, at *12.

[183]. *See Id.* (although Judge Patel did dismiss the screening and marketing representation claim).

[184]. *See Mazur*, 2008 WL 618988.

[185]. *See Id.* at *9.

[186]. *See* Band, *supra* note 11; Finn *et. al., supra* note 48, at 351.

[187]. *See, e.g*. Band, *supra* note 11, at 3; 47 U.S.C. § 230(b)(4).

[188]. Goldman, *supra* note 112.

[189]. *Id.*

[190]. Anne Keaty, J.D., Roger J. Johns, J.D., LL.M., and Lucy L. Henke, Ph.D. *Can Internet Service Providers and Other Secondary Parties Be Held Liable for Deceptive Online Advertising?*, 58 Bus. Law 479, 484, 493 (2002-2003) (In passing the FTCA, Congress gave the FTC the right to regulate unfair methods of competition, including unfair or deceptive acts or practices (e.g., deceptive advertising)).

[191]. *Id.* at 493.

[192]. *Id.* at 493-94 (citing Federal Trade Commission, *Dot Com Disclosures*, at pt. III (2000), available at http:// www.ftc.gov/bcp/edu/pubs/business/ecommerce/bus41.pdf).

[193]. *Id*. at 495 (citing Federal Trade Commission, *Dot Com Disclosures*, at text accompanying n.18 & pt. III B-C (2000), http:// www.ftc.gov/bcp/conline/pubs/buspubs/ruleroad.htm).

[194]. *Id.* at 498 (citing Federal Trade Commission, Dot Com Disclosures, at pt. II (2000), available at http:// www.ftc.gov/bcp/edu/pubs/business/ecommerce/bus41.pdf).

[195]. *Id.* at 494 (citing Federal Trade Commission, Dot Com Disclosures, at pts. III A, B (2000), available at http://www.ftc.gov/bcp/edu/pubs/business/ecommerce/bus41.pdf).

[196]. *See Id.* at 499.

[197]. *See Id.*

[198]. *See* 47 U.S.C. 230(e)(3) (commenting on safe harbor effects on state law but not federal law). The effect of CDA § 230 on federal laws is uncertain, as two circuits have issued contrasting opinions on the safe harbor's effect on the Fair Housing Act. In *Chicago Lawyers' Committee for Civil Rights Under Law, Inc. v. Craigslist, Inc.*, 519 F.3d 666(7th Cir. 2008), CDA § 230 immunized the defendant from FHA claims, but in *Fair Housing Council of San Fernando Valley v. Roommates.com, LLC*, 521 F.3d 1157 (9th Cir. 2008), the defendant was denied CDA § 230 immunity from FHA claims.

[199]. Keaty et. al., *supra* note 190, at 508.

[200]. *See Mazur*, 2008 WL 618988, at *12.

[201]. *See Id.*

[202]. *See* Finn *et. al., supra* note 48, at 371.

[203]. *See* 47 U.S.C. § 230(b)(2).

[204]. *See Blumenthal*, 992 F. Supp. at 48 n. 7.

[205]. *See* 47 U.S.C. § 230(b)(2).

[206]. *See* Band, *supra* note 11, at 3.

[207]. Global Business Dialogue on Internet Commerce, http://www.gbde.org.

[208]. *Id.*

[209]. *Id.*

[210]. Global Business Dialogue on Internet Commerce, Consumer Confidence, http://www.gbd-e.org/ig/cc_top.html.

[211]. Global Business Dialogue on Internet Commerce, http://www.gbd.org

[212]. *Id.*

[213]. Favre, *supra* note 31, at 207-08 (members include Hewlett-Packard, IBM, and Apple Computer); *see* http://www.siia.net.

[214]. *Id.*

[215]. *See Id.*

[216]. *See* Finn *et. al., supra* note 48, at 348-49.

[217]. *See Id.*

[218]. *See* Rustad, *supra* note 12, at 67.

[219]. *See* Global Business Dialogue on Internet Commerce, http:// www.gbde.org.

[220]. *See* Finn *et. al., supra* note 48, at 366.

[221]. *Id.* at 372.

[222]. *Id.*

[223]. *See Mazur*, at 12-13 (eBay user agreement was unconscionable).

[224]. *See* Rustad, *supra* note 12.

[225]. Favre, *supra* note 31, at 172-77.

[226]. *Id.* at 189-96; *See also Tiffany, Inc, v. Ebay, Inc.*, 576 F.Supp.2d 463 (S.D.N.Y. 2008) (noting that reasoning in *Gentry* case related to CDA § 230 was instructive, and stating "it cannot be said that eBay was misleading customers when eBay was diligently removing listings from the website that were purportedly counterfeit.")

[227]. *See Id.* at 196.

[228]. 47 U.S.C. § 230(b)(1).

The imposition of tort liability on service providers for the communications of others represented, for Congress, simply another form of intrusive government regulation of speech. 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 other parties' potentially injurious messages. Id. at 330-31 (emphasis added). The Zeran quotation, in context, refers to defamation and other forms of tort liability.Â I have just modified 2 external links on Section 230 of the Communications Decency Act. Please take a moment to review my edit. If you have any questions, or need the bot to ignore the links, or the page altogether, please visit this simple FaQ for additional information. Section 230 of the Communications Decency Act of 1996 (a common name for Title V of the Telecommunications Act ofÂ In Zeran v. America Online, Inc., the Court notes that "Congress enacted Â§ 230 to remove the disincentives to self-regulation created by the Stratton Oakmont decision. [4] Under that court's holding, computer service providers who regulated the dissemination of offensive material on their services risked subjecting themselves to liability, because such regulation cast the service provider in the role of a publisher.Â The bill clarifies the country's sex trafficking law to make it illegal to knowingly assist, facilitate, or support sex trafficking, and amends the Section 230 safe harbors of the Communications Decency Act (which make online section 230 of the Communications Act of 1934 (47 U.S.C. 230; commonly known as the â€˜Communications Decency Act of 1996â€™) was never intended to provide legal protection to websites that unlawfully promote and facilitate prostitution and websites that facilitate traffickers in advertising the sale of unlawful sex acts with sex trafficking victimsÂ The growth of online platforms in recent years raises important questions about applying the ideals of the First Amendment to modern communications technology. Today, many Americans follow the news, stay in touch with friends and family, and share their views on current events through social media and other online platforms. As a result, these platforms function in many ways as a 21st century equivalent of the public square.