BADGING: SECTION 230 IMMUNITY IN A WEB 2.0 WORLD

The drafters of § 230 of the Communications Decency Act[1] (CDA) aimed to encourage the growth of free speech online while also giving site operators an incentive to edit and self-police by granting those owners immunity from liability for content posted by nonowner users, even when the owners attempt to monitor their sites for harmful content.[2] In the fourteen years since the enactment of the CDA, the immunity provision has been critical to the development of free, open speech online. But there are serious questions about how § 230 immunity should apply to today's more interactive websites, often called Web 2.0.[3] Concerns about whether § 230 will apply to Web 2.0 sites (and whether it should) have increased in the wake of the Ninth Circuit's recent decision in *Fair Housing Council of San Fernando Valley v. Roommates.com, LLC*,[4] which put a partial stop to a chain of court decisions expanding the application of § 230. This Note extends this discussion to the specific issue of § 230 immunity for Web 2.0 sites that "badge" certain users with a symbol of a special status.[5]

The concept of Web 2.0 is "a bit of a muddle."[6] One element is the emergence of a more interactive internet, where the line between user and contributor is blurred or nonexistent and sites have "embraced the power of the web to harness collective intelligence."[7] It is the internet of blogs, of wikis, of user-generated reviews and information. In a world where everyone can participate, users need some way of sorting all of the information that is produced, a way to determine both what

---

[1] 47 U.S.C. § 230 (2006).

[2] *See* Batzel v. Smith, 333 F.3d 1018, 1027–28 (9th Cir. 2003) (examining the history of the section).

[3] *See, e.g.*, H. Brian Holland, *In Defense of Online Intermediary Immunity: Facilitating Communities of Modified Exceptionalism*, 56 U. KAN. L. REV. 369 (2008); Eric Weslander, Comment, *Murky "Development": How the Ninth Circuit Exposed Ambiguity Within the Communications Decency Act, and Why Internet Publishers Should Worry*, 48 WASHBURN L.J. 267, 296 (2008); Cecilia Ziniti, Note, *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 (2008).

[4] 521 F.3d 1157 (9th Cir. 2008) (en banc).

[5] *See, e.g.*, Amazon.com, Badges, http://www.amazon.com/gp/help/customer/display.html/ref=cm_rn_bdg_help?ie=UTF8&nodeId=14279681&pop-up=1#VN (last visited Jan. 9, 2010) ("[B]adges are a great way for customers to identify our best content contributors."); Posting of LeslieMiller to Symantec Connect, http://www.symantec.com/connect/blogs/what-trusted-advisor (Mar. 27, 2009) ("Trusted Advisors are identified in the community with a special badge and are the front line of support for community users. Trusted Advisors are not Symantec Corp. employees.").

[6] The Long Tail, http://www.thelongtail.com/the_long_tail/2005/10/web_20_and_the_.html (Oct. 1, 2005, 11:13).

[7] Tim O'Reilly, *What Is Web 2.0: Design Patterns and Business Models for the Next Generation of Software*, O'REILLY, Sept. 30, 2005, http://oreilly.com/lpt/a/6228.

information is relevant and what is credible.[8] One way websites accomplish this task is through the "badging" of users, the use of a symbol or word to distinguish people as trusted, experienced members of the community or as administrators of the site.[9]

This Note examines two badge-related problems. First, for badges that indicate a poster's quality, it examines the possibility of a site being sued for negligent misrepresentation. Second, for badges that indicate administrative rights, it examines the possibility of a site being sued for posts made by administrative users in a nonadministrative capacity. Since § 230's goal is to encourage self-editing and internet free speech, the section should continue to be interpreted broadly, and mere badging of a user should not deprive an interactive computer service provider of immunity for most user torts. In particular, site owners should be protected from liability for the torts of users whom, with regard to badges indicating quality, the site owner did not select, or of users who, with regard to administrative badges, were not acting within the scope of their employment.

Part I examines the history of § 230, specifically Congress's intent to encourage free speech online and to encourage interactive computer services and users to self-police, as well as scholars' and courts' reactions to the provision. Part II discusses the application of § 230 in a Web 2.0 world and the use of badges. Part III examines the two above-mentioned badge-related problems and suggests that they should be resolved by restricting the *Roommates.com*[10] holding to its facts and continuing the earlier trend of broad interpretation of § 230. Part IV briefly concludes.

I. SECTION 230: HISTORY AND REACTION

A. The Purpose and History of § 230

In enacting the CDA,[11] Congress created § 230 explicitly "to encourage the unfettered and unregulated development of free speech on

---

[8] *See* YOCHAI BENKLER, THE WEALTH OF NETWORKS 68 (2006).

[9] The term "badge" is also used in the online context to refer to "a small image used on websites to promote web standards, products used in the creation of a web page or product, or to indicate a specific content license that is applied to the content or design of a website." Wikipedia, Web Badge, http://en.wikipedia.org/wiki/Web_badge (last visited Jan. 9, 2010). This Note does not analyze such badges.

[10] "[T]he company goes by the singular name 'Roommate.com, LLC' but pluralizes its website's URL." Fair Hous. Council of San Fernando Valley v. Roommates.com, LLC, 521 F.3d 1157, 1161 n.2 (9th Cir. 2008) (en banc). For consistency, this Note will refer to this case as *Roommates.com* throughout.

[11] The bulk of the CDA, which restricted minors' access to indecency, was struck down as a violation of the First Amendment in *Reno v. ACLU*, 521 U.S. 844 (1997).

the Internet, . . . promote the development of e-commerce,"[12] and "encourage interactive computer services and users of such services to self-police the Internet for obscenity and other offensive material, so as to aid parents in limiting their children's access to such material."[13] Under the section's immunity provision, also known as its "Good Samaritan" section, "[n]o provider or user of an interactive computer service [is] treated as the publisher or speaker of any information provided by another information content provider."[14] An "interactive computer service" is defined as "any information service, system, or access software provider that provides or enables computer access by multiple users to a computer server, including specifically a service or system that provides access to the Internet and such systems operated or services offered by libraries or educational institutions."[15] 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."[16] Section 230 was added relatively late in the drafting process as a response[17] to a New York State case, *Stratton Oakmont, Inc. v. Prodigy Services Co.*,[18] in which the court found that Prodigy could be held liable for libelous statements posted on one of its message boards by an anonymous user.[19]

In the first case to interpret the section, *Zeran v. America Online, Inc.*,[20] the Fourth Circuit made clear that § 230 immunized interactive computer services from liability for all acts in "the role of a traditional publisher" — decisions about "whether to publish, edit, or withdraw [a] posting."[21] The court ruled that sites do not become liable if they

---

[12] Batzel v. Smith, 333 F.3d 1018, 1027 (9th Cir. 2003); *see also* 47 U.S.C. § 230 (2006) ("The Internet . . . offer[s] a forum for a true diversity of political discourse, unique opportunities for cultural development, and myriad avenues for intellectual activity. . . . It is the policy of the United States . . . to promote the continued development of the Internet.").

[13] *Batzel*, 333 F.3d at 1028; *see also* 47 U.S.C. § 230(b) ("It is the policy of the United States . . . to encourage the development of technologies which maximize user control over what information is received by [people] who use the Internet . . . [and] to remove disincentives for the development and utilization of blocking and filtering technologies.").

[14] 47 U.S.C. § 230(c)(1).

[15] *Id.* § 230(f)(2).

[16] *Id.* § 230(f)(3).

[17] *See* H.R. REP. NO. 104-458, at 194 (1996) (Conf. Rep.), *reprinted in* 1996 U.S.C.C.A.N. 124, 208 ("One of the specific purposes of this section is to overrule *Stratton-Oakmont v. Prodigy* . . . ."). The Ninth Circuit suggested that the provision may also have been a response to concerns among members of Congress that most of the CDA would be struck down as unconstitutional. *See Batzel*, 333 F.3d at 1028 n.11.

[18] No. 031063/94, 1995 WL 323710 (N.Y. Sup. Ct. May 24, 1995).

[19] *Id.* at *1–4.

[20] 129 F.3d 327 (4th Cir. 1997).

[21] *Id.* at 332; *see also* Ben Ezra, Weinstein & Co. v. Am. Online Inc., 206 F.3d 980, 986 (10th Cir. 2000).

refuse to take a post down upon receiving notice of its tortious content.[22] The panel reasoned that "[i]f computer service providers were subject to distributor liability, they would face potential liability each time they receive notice of a potentially defamatory statement — from any party, concerning any message."[23] The court worried this would encourage interactive computer services to simply delete all messages about which they received notice and avoid any attempts at self-regulation.[24]

In the cases that have followed, § 230 has continued to thrive, with courts broadly interpreting the section's language concerning the parties protected by the immunity provisions. While the passage of § 230 was motivated by fears about liability for internet service providers, § 230 has been found to apply to protect individual websites as well, because § 230 "confers immunity not just on 'providers' of [interactive computer] services, but also on 'users' of such services,"[25] and a website "*must* access the Internet through some form of 'interactive computer service'" in order to be available to the world.[26] As a result, § 230 has been found to give immunity to operators of social networking sites,[27] online dating services,[28] search engines,[29] message boards,[30] and shopping services.[31] While it appears there has been no reported decision directly addressing immunity for blogs, courts and litigants have seemed at times to assume blogs are covered by § 230 immunity[32] and most of the literature assumes immunity will apply.[33]

Though courts have interpreted § 230 broadly, it is important here to make clear what § 230 does not do — it does not grant immunity to the original posters.[34] Section 230 also explicitly does not provide im-

---

[22] *Zeran*, 129 F.3d at 333.

[23] *Id.*

[24] *Id.*

[25] Batzel v. Smith, 333 F.3d 1018, 1030 (9th Cir. 2003).

[26] *Id.* at 1031.

[27] Doe v. MySpace, Inc., 528 F.3d 413, 422 (5th Cir. 2008).

[28] Carafano v. Metrosplash.com, Inc., 339 F.3d 1119, 1125 (9th Cir. 2003).

[29] Parker v. Google, Inc., 422 F. Supp. 2d 492, 501 (E.D. Pa. 2006).

[30] DiMeo v. Max, 433 F. Supp. 2d 523, 531 (E.D. Pa. 2006).

[31] *E.g.*, Gentry v. eBay, Inc., 121 Cal. Rptr. 2d 703, 715 n.7 (Ct. App. 2002); Schneider v. Amazon.com, Inc., 31 P.3d 37, 40–41 (Wash. Ct. App. 2001).

[32] *See* Doe v. City of New York, 583 F. Supp. 2d 444, 449 (S.D.N.Y. 2008) (noting defendant's argument that "his emails were akin to a blog" and thus deserved immunity); *DiMeo*, 433 F. Supp. 2d at 528 (indicating blogs would need to be highly monitored "absent federal statutory protection").

[33] *See, e.g.*, Melissa A. Troiano, Comment, *The New Journalism?: Why Traditional Defamation Laws Should Apply to Internet Blogs*, 55 AM. U. L. REV. 1447, 1461 (2006); Posting of Jack Balkin to Balkinization, http://balkin.blogspot.com/2003_06_29_balkin_archive.html#105723343690170641 (July 3, 2003, 7:57).

[34] *See* Zeran v. Am. Online, Inc., 129 F.3d 327, 330 (4th Cir. 1997).

munity from intellectual property–related claims[35] or for violations of federal criminal law.[36]

In addition, the most recent important case on § 230, *Roommates.com*, has bucked the trend of expansive interpretations of this section.[37] In order to use the Roommates.com site, which helped users find potential roommates, all users were required to answer questions about their sex, sexual orientation, and whether children would be living with them, as well as what they were looking for in terms of answers to those questions in potential roommates. The site then created user profiles based on this information.[38] Users also had the option of entering additional comments in a box provided for that purpose.[39] The website allowed users of the site to search by various categories and receive emails containing profiles matching their criteria.[40] Two fair housing councils sued Roommates.com,[41] alleging the site was violating the Fair Housing Act[42] (FHA) — which bans discrimination on the basis of, inter alia, sex and familial status[43] — as well as a California statute banning discrimination based on those categories and sexual orientation.[44] The site raised § 230 as a defense, and it was successful before the trial court.[45]

However, the Ninth Circuit ruled that Roommates.com could not claim immunity for parts of its site. First, and less controversially, the court ruled that the site was not immune from suit for asking users questions that potentially violated the FHA and forcing users to answer them, since that process made the site the information content provider for those questions.[46] Second, the court examined the issue of the profiles created from the answers to the questions and the site's search and email features. It ruled that since the website allowed users answering those questions to only choose from a list of possible responses it provided, Roommates.com was "the developer, at least in part, of that information," exposing the site to liability.[47] Along the same lines, the court held that Roommates.com could not claim im-

---

[35] 47 U.S.C. § 230(e)(2) (2006).

[36] *Id.* § 230(e)(1).

[37] *See* Fair Hous. Council of San Fernando Valley v. Roommates.com, LLC, 521 F.3d 1157 (9th Cir. 2008) (en banc).

[38] *Id.* at 1161.

[39] *Id.*

[40] *Id.* at 1162.

[41] *Id.*

[42] 42 U.S.C. §§ 3601–3631 (2006).

[43] *Id.* § 3604(c).

[44] CAL. GOV'T CODE § 12955 (West 2005).

[45] *See* Fair Hous. Council of San Fernando Valley v. Roommate.Com, LLC, No. CV 03-09386PA(RZX), 2004 WL 3799488, at *4 (C.D. Cal. Sept. 30, 2004).

[46] *Roommates.com*, 521 F.3d at 1164–65.

[47] *Id.* at 1166.

munity for its search or email systems since it "designed its search system so it would steer users based on the preferences and personal characteristics that [the site] itself forces subscribers to disclose."[48] Finally, the court ruled that Roommates.com retained immunity for information posted in the comments box, since it is "not responsible, in whole or in part, for the development of this content."[49] The court noted that users could post whatever they wanted in this space, with no shaping of the content by the site, unlike the list of answers to the other questions.[50]

As *Roommates.com* demonstrates, despite the overall trend of expansive interpretations of § 230, the state of the law remains somewhat unsettled, especially in the face of the more interactive Web 2.0. Although a few courts deciding cases post-*Roommates.com* have preserved immunity and limited the case to its facts,[51] more expansive interpretations of the case could still occur. In the wake of *Roommates.com*, courts must continue to be cautious not to retreat to such an extent that the section's purposes are threatened.

B. Reaction to § 230

Some courts and scholars have expressed severe apprehension about the immunity provided by § 230, at least as it has been interpreted by most courts. The Ninth Circuit noted in *Batzel v. Smith*[52] that "the broad immunity created by § 230 can sometimes lead to troubling results," such as providing no incentive for a website owner to take down a post after being informed it is defamatory.[53] Similarly, Professor Ann Bartow has argued that § 230 leaves "Internet harassment victims vulnerable and helpless" because it gives internet service providers "no incentive or obligation" to remove harassing posts.[54] Other scholars have argued that the case law has created "a rather in-

---

[48] *Id.* at 1167.

[49] *Id.* at 1174.

[50] *Id.*

[51] In *Doe v. MySpace Inc.*, 96 Cal. Rptr. 3d 148 (Ct. App. 2009), MySpace was sued after a minor was sexually assaulted by an adult user she met on the site, but the court noted that, while MySpace prompted users to provide personal information and facilitated user searches of this information, the questions MySpace asked were not "discriminatory or otherwise illegal" and users did not have to answer the questions to use the site. *Id.* at 158. The court ruled that MySpace was not an information content provider and was therefore immune under § 230. *Id.* at 158–59; *see also* Doe v. MySpace, Inc., 629 F. Supp. 2d 663, 664 (E.D. Tex. 2009); Atl. Recording Corp. v. Project Playlist, Inc., 603 F. Supp. 2d 690, 701–02 (S.D.N.Y. 2009).

[52] 333 F.3d 1018 (9th Cir. 2003).

[53] *Id.* at 1031 n.19.

[54] Ann Bartow, *Internet Defamation as Profit Center: The Monetization of Online Harassment*, 32 HARV. J.L. & GENDER 383, 418 (2009); *see also* DANIEL J. SOLOVE, THE FUTURE OF REPUTATION 159 (2007).

consistent body of law," treating similar acts in different ways.[55] Moreover, while § 230 does not grant immunity to the original poster, the poster is often hard to find due to the anonymity of the internet and can often be effectively judgment-proof.[56] At the same time, speech on the internet can spread extremely quickly, causing significant damage. As a result, some scholars have suggested major changes to cut back the scope of § 230 immunity. Suggestions range from replacing § 230 with a system in which internet service providers would be required to take down posts constituting cyberbullying upon notice,[57] to amending § 230 to remove immunity when a "blogger actively chose to publish a specific and defamatory third-party message."[58]

However, while some sites have certainly taken unfair advantage of § 230, other scholars and courts have noted that the immunity it provides is critical to allowing the continued growth and development of free speech online. Professor Jack Balkin argues:

> [Section 230] has had enormous consequences for securing the vibrant culture of freedom of expression we have on the Internet today. . . . Because online service providers are insulated from liability, they have built a wide range of different applications and services that allow people to speak to each other and make things together. Section 230 is by no means a perfect piece of legislation; it may be overprotective in some respects and underprotective in others. But it has been valuable nevertheless.[59]

Similarly, Professor John Palfrey, though arguing § 230 should be scaled back in some cases, has "credit[ed] [it] as a cornerstone of the legal framework that has enabled the information technology sector to thrive over the past decade" and noted that it "has also had a crucial part in ensuring that the Internet has become a place where free ex-

---

[55] *See* Posting of Daniel Solove to Concurring Opinions, http://www.concurringopinions.com/archives/2006/11/barrett_v_rosen.html (Nov. 22, 2006, 12:51). For example, a site owner can be sued for writing a post about something a friend told him orally but not for posting an email from that friend containing the same information. *See id.*

[56] *See* Lyrissa Barnett Lidsky, *Silencing John Doe: Defamation & Discourse in Cyberspace*, 49 DUKE L.J. 855, 859 (2000) ("[T]he typical John Doe [defendant] has neither deep pockets nor libel insurance from which to satisfy a defamation judgment."). *But see* Susan W. Brenner, *Criminalizing "Problematic" Speech Online*, J. INTERNET L., July 2007, at 3, 4 (noting that website publishers may also be judgment-proof).

[57] Bradley A. Areheart, *Regulating Cyberbullies Through Notice-Based Liability*, 117 YALE L.J. POCKET PART 41, 43 (2007), http://thepocketpart.org/2007/09/08/areheart.html. Areheart proposes a scheme similar to the notice-and-takedown requirements of the Digital Millennium Copyright Act. *Id.*; *see* 17 U.S.C. § 512(c) (2006); *see also Batzel*, 333 F.3d at 1031 n.19 (suggesting this as a possible solution).

[58] Troiano, *supra* note 33, at 1476.

[59] Jack M. Balkin, *The Future of Free Expression in a Digital Age*, 36 PEPP. L. REV. 427, 434 (2009) (footnotes omitted).

pression, like innovation, also thrives."[60] The Fourth Circuit, reacting to the proposal of a notice-and-takedown system in *Zeran*, noted that such a system would encourage parties merely "displeased" with a user's post to notify the interactive computer service provider that the post was defamatory.[61] The court noted that "[i]n light of the vast amount of speech communicated through interactive computer services, these notices could produce an impossible burden for service providers, who would be faced with ceaseless choices of suppressing controversial speech or sustaining prohibitive liability."[62] Instead, the best way to promote free speech while still protecting people from harmful speech online is to encourage sites to sensibly self-regulate, through badging and similar systems.[63]

Though people can be cruel to one another online, this Note comes down on the side of the importance of immunity. As one court stated more broadly:

> Some of the dialogue on the Internet surely tests the limits of conventional discourse. Speech on the Internet can be unfiltered, unpolished, and unconventional, even emotionally charged, sexually explicit, and vulgar — in a word, "indecent" in many communities. But we should expect such speech to occur in a medium in which citizens from all walks of life have a voice.[64]

Users who commit torts online should be liable for them, but websites should remain free of liability so that everyone's voice can still be heard.

II. SECTION 230 IN A WEB 2.0 WORLD AND "BADGING"

As written, § 230 is premised on a view of the internet as consisting of the interaction of several different types of actors: interactive computer services, users, and information content providers. The section recognizes that one entity can fit into more than one category at once. For example, the immunity provision recognizes that an interactive computer service (or user) can also be an information content provider — immunity is explicitly given only for "information provided by *another* information content provider."[65] If America Online writes something on its own forums, it is liable if that content is defamatory. Similarly, every user is responsible for what he or she individually

---

[60] Adam Thierer & John Palfrey, *Dialogue: The Future of Online Obscenity and Social Networks*, ARS TECHNICA, http://arstechnica.com/tech-policy/news/2009/03/a-friendly-exchange-about-the-future-of-online-liability.ars (last updated Mar. 5, 2009).

[61] Zeran v. Am. Online, Inc., 129 F.3d 327, 333 (4th Cir. 1997).

[62] *Id.*

[63] *See id.* at 331.

[64] ACLU v. Reno, 929 F. Supp. 824, 882 (E.D. Pa. 1996), *aff'd*, 521 U.S. 844 (1997).

[65] 47 U.S.C. § 230(c)(1) (2006) (emphasis added).

writes. The problem is that a Web 2.0 world creates more blurring of these already somewhat fuzzy lines.[66]

A. What is Web 2.0?

"Web 2.0" means different things to different people.[67] Some criticize the entire idea as "marketing hype."[68] But Tim O'Reilly, the founder of a computer book publishing company and popularizer of the term, has defined the term this way:

> Web 2.0 is the business revolution in the computer industry caused by the move to the internet as platform, and an attempt to understand the rules for success on that new platform. Chief among those rules is this: Build applications that harness network effects to get better the more people use them.[69]

What makes this innovation important for the purpose of this Note is the shift in the internet from something people merely look at and read to something they truly interact with and change.[70] As *Time* magazine recognized in declaring "You" its Person of the Year in 2006:

> [This is] [n]ot the Web that Tim Berners-Lee hacked together . . . as a way for scientists to share research. It's not even the overhyped dotcom Web of the late 1990s. The new Web is a very different thing. It's a tool for bringing together the small contributions of millions of people and making them matter. Silicon Valley consultants call it Web 2.0, as if it were a new version of some old software. But it's really a revolution.[71]

It is the blogger conversing from the computer in her apartment with users from around the world sitting in front of theirs, the historian who scours articles in Wikipedia with a fine-toothed comb for errors, the antivirus expert who spends hours each day helping people he will never meet solve their problems on a message board, the citizen journalist capturing a video with his cell phone and posting it online for all

---

[66] *See* Posting of Daniel Solove to Concurring Opinions, http://www.concurringopinions.com/archives/2008/04/fair_housing_co.html (April 5, 2008, 10:55) (noting a "major difficulty with applying § 230 to some Web 2.0 applications — it is often hard to figure out exactly who is responsible for providing content"); *see also* 47 U.S.C. § 230(f)(3) (noting that an entity is an information content provider if it is "responsible, in whole or in part, for the creation or development of information").

[67] *See* Ongoing, http://www.tbray.org/ongoing/When/200x/2005/08/09/Web-2.0 (Aug. 9, 2005) ("'Web 2.0' means, well, anything you want it to.").

[68] Ongoing, http://www.tbray.org/ongoing/When/200x/2005/08/04/Web-2.0 (Aug. 4, 2005); *cf.* Scott Laningham, *developerWorks Interviews: Tim Berners-Lee*, IBM DEVELOPERWORKS, Aug. 22, 2006, http://www.ibm.com/developerworks/podcast/dwi/cm-into82206txt.html ("Web 2.0 is, of course, a piece of jargon, nobody even knows what it means.").

[69] *See* Posting of Tim O'Reilly to O'Reilly Radar, http://radar.oreilly.com/archives/2006/12/web-20-compact.html (Dec. 10, 2006) (emphasis omitted).

[70] *See* Enterprise Web 2.0, http://blogs.zdnet.com/Hinchcliffe/?p=41 (May 15, 2006, 10:42) ("Read-write Web + People Using It = Web 2.0.").

[71] Lev Grossman, *Time Person of the Year: You*, TIME, Dec. 25, 2006, at 40.

to see. When exactly this shift happened is somewhat in dispute.[72] But it is hard to argue against "the widespread sense that there's something qualitatively different about today's web."[73]

Of course, while Web 2.0 is a world in which it is easier for people to collectively do great good, it is also a world in which it is possible for people to do great harm. The thousands of people posting each day on a collaborative blog add thousands of voices to the discussion, but also represent thousands of potential tortfeasors. The antivirus expert may just as easily give bad advice that destroys a user's computer as good advice that saves it. "Web 2.0 harnesses the stupidity of crowds as well as [their] wisdom."[74]

As a result, § 230 has a major role to play in this world. Indeed, without § 230, Web 2.0 may not have even come into existence.[75] For example, Professor H. Brian Holland has written of the "important role § 230 plays in the development of online communities"[76] — it allows communities to develop "by substantially and continually mitigating the primacy of external legal norms within the confines of the community."[77] Holland also argues that Web 2.0 communities actually further the end of § 230 by allowing users to choose between values while the site's operator "retains control over the architecture and thus the means of enforcement."[78]

B. Badging

The problem with a world in which everyone can get involved in the discussion is that it can be difficult to manage and difficult to determine whose posts are relevant, informative, correct, or particularly helpful. Professor Yochai Benkler, in his important work *The Wealth of Networks*,[79] describes two different necessary elements to sorting all of this information produced online: relevance and credibility.[80] As Benkler notes in an earlier law review article on the same topic, "Who in their right mind wants to get answers to legal questions from a fifteen-year-old child who learned the answers from watching Court

---

[72] O'Reilly dates it as occurring after the collapse of the dot com bubble in the fall of 2001. *See* O'Reilly, *supra* note 7.

[73] Posting of Tim O'Reilly to O'Reilly Radar, http://radar.oreilly.com/archives/2005/08/not-20.html (Aug. 5, 2005).

[74] Grossman, *supra* note 71, at 41.

[75] *See* Posting of Adam Thierer to The Technology Liberation Front, http://techliberation.com/2009/01/13/web-20-section-230-and-nozicks-utopia-of-utopias (Jan. 13, 2009) (arguing that "Section 230 has been instrumental in fostering and protecting" the development of Web 2.0).

[76] Holland, *supra* note 3, at 404.

[77] *Id.* at 397.

[78] *Id.* at 399.

[79] *See* BENKLER, *supra* note 8.

[80] *Id.* at 68.

TV?"[81] Relevance and credibility can be achieved by "harnessing the users themselves."[82] Sites can help users find credible and relevant information through user accreditation, either by those users' fellow users[83] or by site administrators.

In many cases, this accreditation takes the form of "badging" — the placement of a recognizable symbol, word, or icon next to the person's username. Sites can use stars, points, or other symbols.[84] As one website's description of its badges notes:

> Most badges (bling) are a sign of respect, honesty[,] knowledge, trustworthey'ness [sic], etc. As silly as those little things are, they are the only thing that most members can use to decide how much credibility another member has. Because our site is "for beginners" it is important to know who can be trusted to give good, useful help or information.[85]

Exactly how a badge is obtained varies. Some sites award special status through consensus.[86] In others, users obtain a badge by being recognized by their peers.[87] In still others, the site's operator makes the decision about whom to promote. Of course, not every badge means the same thing. On some sites, badges are used to identify users who are known for adding particularly helpful information to a discussion (or at least users who post frequently). On others, badges identify users with special administrative rights, such as the ability to edit others' posts, move posts from one place to another, delete libelous or offensive posts, and generally guide and moderate the site.

While badges serve an important function, they also expose site owners to potential liability. The fact that a user has been helpful or trustworthy in the past does not mean she will not commit a tort in the future. The next Part of this Note examines how site owners could be held liable for their badged users' acts.

---

[81] Yochai Benkler, *Coase's Penguin, or, Linux and* The Nature of the Firm, 112 YALE L.J. 369, 390–91 (2002); *see also* MICHAEL LEWIS, NEXT: THE FUTURE JUST HAPPENED 104 (2002).

[82] BENKLER, *supra* note 8, at 75.

[83] Benkler, *supra* note 81, at 391–96.

[84] For an example of the many varieties of badges, see Grown Up Geek, How The Badging System Works, http://grownupgeek.com/grown-up-geek-badges (last visited Oct. 22, 2009).

[85] Posting of hubby to Grown Up Geek, http://grownupgeek.com/how-to-lose-your-bling (Dec. 27, 2006, 15:03) (emphasis omitted).

[86] *See* Wikipedia, Wikipedia: Administrators, http://en.wikipedia.org/wiki/Wikipedia:Administrators (last visited Jan. 9, 2010).

[87] Posting of Animal to Bleeping Computer, http://www.bleepingcomputer.com/forums/topic80359.html (Feb. 5, 2007, 12:05) ("Bleeping Computer Advisors are regular forum contributors who have been nominated by their peers or other members of the staff as a result of their consistently high quality and expert responses to people's questions in the forums; Advisors can be trusted to give correct and understandable answers to our member['s] questions.").

III. TWO PROBLEMS INVOLVING BADGING AND § 230

This Note examines two distinct problems involving § 230, one for each of the primary roles for which badges are used. The first, involving badges that identify helpful users, is what this Note will refer to as the "Good Housekeeping Seal" problem — a site's perceived "endorsement and approval" of users who wear a badge and the potential resulting liability for negligent misrepresentation.[88] The second, involving badges identifying administrators, is an agency problem — a site's perceived liability for the posts of users identified as administrators but whose posts were made in a capacity unrelated to that role.

A. Endorsement: The Good Housekeeping Seal Problem

Under the tort of negligent misrepresentation, one can be liable for "suppl[ying] false information for the guidance of others . . . if he fails to exercise reasonable care or competence in obtaining or communicating the information" and another individual justifiably relies on the information.[89] Normally, site owners would have little to fear about a negligent misrepresentation claim. They are not generally liable for false information supplied by their users under § 230. And even without § 230, publishers generally have "no liability for negligent publication of erroneous information."[90]

However, courts have carved out an exception to this general rule, imposing liability for a publisher's negligent endorsement.[91] If a badge describing a poster's quality functions as a similar endorsement, website owners could be liable if the poster they endorsed then caused damage. A "leading case"[92] on the issue of negligent endorsement from the pre-internet era is a decision from the California Court of Appeal, *Hanberry v. Hearst Corp.*[93]

On March 30, 1966, Zayda Hanberry slipped and fell while wearing a pair of shoes she alleged were defective because they were slippery when worn on a vinyl surface.[94] The shoes had been advertised

---

[88] *See* Hanberry v. Hearst Corp., 81 Cal. Rptr. 519 (Ct. App. 1969). There is at least one case of a website being sued for negligent misrepresentation. *See* Anthony v. Yahoo! Inc., 421 F. Supp. 2d 1257, 1262–63 (N.D. Cal. 2006).

[89] RESTATEMENT (SECOND) OF TORTS § 552(1) (1977). The defendant's liability in such a case is limited to a person or small group of persons for "whose benefit and guidance he intends to supply the information or knows that the recipient intends to supply it; and . . . through reliance upon it in a transaction that he intends the information to influence or knows that the recipient so intends or in a substantially similar transaction." *Id.* § 552(2).

[90] 2 ROBERT D. SACK, SACK ON DEFAMATION § 13.8, at 13-60 (3d ed. 2004).

[91] *See Hanberry*, 81 Cal. Rptr. at 521.

[92] Nicolas P. Terry, *Cyber-Malpractice: Legal Exposure for Cybermedicine*, 25 AM. J.L. & MED. 327, 357 n.253 (1999).

[93] 81 Cal. Rptr. 519.

[94] *Id.* at 521.

in Hearst Corporation's *Good Housekeeping* magazine as receiving the "Good Housekeeping's Consumers' Guaranty Seal," which the magazine claimed was given only after the magazine "satisf[ied itself] that [the] products . . . are good ones and that the advertising claims made for them in [the] magazine are truthful."[95] Hanberry sued Hearst on a theory of, inter alia, negligent misrepresentation.[96] The court was faced with the question of "whether one who endorses a product for his own economic gain, and for the purpose of encouraging and inducing the public to buy it, may be liable to a purchaser who, relying on the endorsement, buys the product and is injured because it is defective and not as represented."[97]

The court held that Hearst could be liable.[98] It reasoned that Hearst was using the seal to "enhance the value of its magazine as an advertising medium, to compete more favorably in the advertising market."[99] "Implicit in the seal and certification is the representation respondent has taken reasonable steps to make an independent examination of the product endorsed, with some degree of expertise, and found it satisfactory," the court concluded.[100] "Since the very purpose of respondent's seal and certification is to induce consumers to purchase products so endorsed, it is foreseeable certain consumers will do so."[101] As a result, Hearst had a duty to use ordinary care in deciding which products could bear the Good Housekeeping Seal.[102]

Courts have limited *Hanberry*'s reach in several more recent cases. The most relevant to this analysis is *Yanase v. Automobile Club of Southern California*.[103] In *Yanase*, the widow of a man killed in the parking lot of a hotel sued the publisher of a Tourbook that had rated the hotel, alleging negligent misrepresentation.[104] The widow alleged that her husband had "relied on [the book] in selecting the motel and he would not have selected the motel if Auto Club had determined it was in a high crime area and offered inadequate security, published this information in the Tourbook, or not recommended the motel at all."[105] The court found that "the *Hanberry* decision furnishes no support for Yanase's position."[106] First, it noted that there was "nothing

---

95 *Id.* (internal quotation mark omitted).
96 *Id.*
97 *Id.*
98 *Id.*
99 *Id.* at 522.
100 *Id.*
101 *Id.*
102 *Id.*
103 260 Cal. Rptr. 513 (Ct. App. 1989).
104 *Id.* at 514.
105 *Id.* at 515–16.
106 *Id.* at 519.

in the Auto Club's Tourbook listing or rating that consists of a positive assertion [or implication] concerning neighborhood safety or the security measures taken in connection with the motel."[107] The book only rated the hotel's accommodations and, since they were as described, the court held that there were no misrepresentations and *Hanberry* did not apply.[108] Second, the court wrote that there was not a "very close relationship between the injury and the product when put to ordinary use within the scope of the endorsement."[109] Finally, the court distinguished *Hanberry*'s negligent misrepresentation claim, which was close to a products liability cause of action, from Yanase's claim, which was analogous to a premises liability case.[110]

The questions, then, in regard to potential liability for badges are whether a badge is akin to the Good Housekeeping Seal and, therefore, whether a site that provides such a badge could be liable for negligent misrepresentation.[111] Under *Hanberry*, to determine whether a party owes a duty of care, a court balances various policy factors, including "the foreseeability of harm to [the plaintiff], the degree of certainty that the plaintiff suffered injury, the closeness of the connection between the defendant's conduct and the injury suffered, the moral blame attached to the defendant's conduct, and the policy of preventing future harm."[112] In the case of a badged user, the court would likely find that harm was highly foreseeable, at least in certain contexts. Imagine, for example, a message board that helped users solve their antivirus problems, or better still, one dealing with personal health. Certainly a site owner could foresee a viewer relying more readily on the advice of a badged user in such a forum; such overreliance could result in harm to that viewer. Similarly, there is a close connection between the site's conduct (directing users to advice on solving their respective computer or health problems) and an injury. Whether the court would attach moral blame to the site's badging might depend on exactly what the badge said. For example, if the badge merely said the user had been active on the site for a long time, that statement would probably not be sufficient to impose liability. Conversely, if a badge indicated a member is "generally trustwor-

---

[107] *Id.* at 516.

[108] *Id.* at 519.

[109] *Id.*

[110] *Id.*

[111] Plaintiffs have sued providers of interactive computer services for negligent misrepresentation in slightly different contexts. *See* Doe v. MySpace, Inc., 474 F. Supp. 2d 843, 852 (W.D. Tex. 2007) (dismissing negligent misrepresentation claim for failure to meet the heightened pleading standard of FED. R. CIV. P. 9(b)).

[112] Hanberry v. Hearst Corp., 81 Cal. Rptr. 519, 522–23 (Ct. App. 1969) (quoting Biakanja v. Irving, 320 P.2d 16, 19 (Cal. 1958)) (internal quotation marks omitted).

thy . . . and probably know[s] what [he is] talking about,"[113] there would be a much higher chance that liability would attach.

It seems likely that *Yanase* does not in itself prevent liability from attaching for a site's badging, though it certainly limits when a site would be liable in several ways. First, liability for badges would likely only attach for badges that directly asserted or implied that the user should be relied upon, distinguishing between the badge awarded for trustworthiness and one awarded just for being a long-time user, as discussed above. Second, there would have to at least be a close relationship between the purpose of the endorsement and the injury. So if the badge indicated the user was especially skilled at solving computer problems, there would be no liability if that user gave advice on a medical issue. Finally, *Yanase* could limit the imposition of liability for certain torts.

Since there is potential liability for websites that badge, the question then becomes whether § 230 applies. As discussed above, § 230 protects the "provider or user of an interactive computer service [from being] treated as the publisher or speaker of any information provided by another information content provider." However, the "information" in this context is the badge itself and the perceived endorsement that results, not the content of the post by the badged user.[114] The badge and the endorsement, in other words, are *not* "information provided by another information content provider." This distinction also suggests that the type of badge at issue may affect the application of § 230: Is the badge awarded by the site's owner? Or is the badge provided by some procedure outside of the owner's direct control? For badges directly awarded by the site's owner, such as Amazon.com's badge verifying that a person is "the" celebrity of that name, the resolution seems to be easier — the "information" would not be supplied by another information content provider, so there would be no immunity.[115]

The more difficult case is one in which the badge was awarded in some other way, say based on the ratings of other users or some sort of automated procedure. One court has ruled directly on this issue. In *Gentry v. eBay, Inc.*,[116] a California intermediate appellate court considered, inter alia, the question of the popular auction site's liability for its safety program. The safety program consists of color-coded stars

---

[113] Grown Up Geek, *supra* note 84.

[114] The site's owner is clearly immunized from liability for the content of the post, since it would not be the creator in whole or in part of that content.

[115] *Cf.* Mazur v. eBay Inc., No. C 07-03967 MHP, 2008 WL 618988, at *10 (N.D. Cal. Mar. 4, 2008) (finding actionable eBay's affirmative statement that its live auctions were "safe"). Of course, the lack of immunity does not necessarily mean the site would ultimately be held liable, just that it would have to defend the suit on its merits.

[116] 121 Cal. Rptr. 2d 703 (Ct. App. 2002).

displayed next to a user's name if that user has received a sufficient level of "Positive Feedback" from other users and a "Power Sellers endorsement" awarded based on sales volume and feedback ratings.[117] The court ruled that, since "the star symbol and 'Power Sellers' designation [are] simply [representations] of the amount of such positive information received by other users of eBay's web site . . . enforcing appellants' negligence claim would place liability on eBay for simply compiling false and/or misleading content created by" third parties.[118] This safety program is effectively a badging system based on other users' ratings.

The potential problem is that *Gentry* was handed down before *Roommates.com*. As Judge McKeown's partial concurrence and partial dissent in *Roommates.com* indicates, the Ninth Circuit "dramatically altered the landscape of Internet liability."[119] Judge McKeown explicitly cited *Gentry* as a prior case that found that "the CDA does not withhold immunity for the encouragement or solicitation of information."[120]

There is certainly language in the *Roommates.com* decision that could encompass badges used to indicate user quality. The *Roommates.com* court found that each user's profile page was at least partially Roommates.com's responsibility, "because every such page is a collaborative effort between [the site] and the subscriber."[121] The court paid special attention to the site's search system and its email notification system, noting that Roommates.com "designed its search system so it would steer users based on the preferences and personal characteristics that [the site] itself forces subscribers to disclose."[122] It held that "a website helps to develop unlawful content, and thus falls within the exception to section 230, if it contributes materially to the alleged illegality of the conduct."[123]

A plaintiff relying on the *Roommates.com* decision would likely argue that a site's owner was the information content provider because it developed the systems that let a badge be awarded and displayed the badge on its site, just as Roommates.com was the information content provider of the questions and choice of answers,[124] the display of profile pages,[125] and its search and email systems that filtered list-

---

117 *Id.* at 717.

118 *Id.* at 717–18.

119 Fair Hous. Council of San Fernando Valley v. Roommates.com, LLC, 521 F.3d 1157, 1176 (9th Cir. 2008) (en banc) (McKeown, J., concurring in part and dissenting in part).

120 *See id.* at 1185 (citing *Gentry*, 121 Cal. Rptr. 2d at 718).

121 *Id.* at 1167 (majority opinion).

122 *Id.*

123 *Id.* at 1168.

124 *Id.* at 1165.

125 *Id.*

ings.[126] Each badge displayed on a website is a collaborative effort between the site and the site's users: the site's owner decides what kind of badges may be displayed, and the users, through voting or their own posting, cause the badge to be displayed. Similarly, the badges are in most cases designed to steer users, even if not in nearly as coercive a way as in *Roommates.com*. The court could hold that a website helps to develop tortious content (here analogous to the "illegal conduct" in *Roommates.com*), and thus falls within the exception to § 230, if it contributes materially to the alleged tortious nature of the conduct — in this case, developing and displaying a badge.

Courts should not make this leap. They should uphold *Gentry*, limit the holding of the Ninth Circuit's *Roommates.com* decision to its facts, and not extend the decision's language on liability to include voluntary systems for the recognition of better users. Indeed, the *Roommates.com* court, in dicta, stated:

> [If] a plaintiff would bring a claim under state or federal law based on a website operator's passive acquiescence in the misconduct of its users, the website operator would likely be entitled to CDA immunity. This is true even if the users committed their misconduct using electronic tools of general applicability provided by the website operator.[127]

The Tenth Circuit recently made a ruling on similar lines, holding that "a service provider is 'responsible' for the development of offensive content only if it in some way specifically encourages development of what is offensive about the content."[128]

The consistent theme of the Tenth Circuit opinion and other recent cases is that what matters is not whether the information displayed is a collaborative effort of some sort; if it were, every Web 2.0 site would lose immunity in a post-*Roommates.com* world. Nor is it whether the system design steers users to offensive conduct. What is key is whether the system itself is designed to facilitate wrongful conduct. Badges are designed to improve the reliability of information by recognizing better users. The information provided or facilitated by the site is about the popularity or approval rating of a user, not something tortious. As such, badges are usually "electronic tools of general applicability" rather than electronic tools facilitating tortious conduct, and their use should not result in the elimination of immunity.

B. The Entity/Agency Problem

The second problem is the issue of users badged with administrative responsibility committing torts while acting in a nonadministra-

---

[126] *Id.* at 1167.
[127] *Id.* at 1169 n.24.
[128] FTC v. Accusearch Inc., 570 F.3d 1187, 1199 (10th Cir. 2009).

tive capacity. Many message boards badge certain users as administrators.[129] In most cases, these users with administrator badges are some of the longest standing, most active, best respected community members on a given site. And they ordinarily participate in the site beyond just their administrative responsibilities. The question here is whether a badged administrator "counts as [part of] the 'person or entity' whose actions the court should analyze in determining whether [a site] is the 'information content provider.'"[130] Like previous work, this Note analyzes this issue using agency principles.[131]

Under the Restatement (Third) of Agency, agency is defined as "the fiduciary relationship that arises when one person (a 'principal') manifests assent to another person (an 'agent') that the agent shall act on the principal's behalf and subject to the principal's control, and the agent manifests assent or otherwise consents so to act."[132] An agent is an "employee" if the "principal controls or has the right to control the manner and means of the agent's performance of work."[133] A principal is vicariously liable "for a tort committed by its employee acting within the scope of employment," which includes "performing work assigned by the employer or engaging in a course of conduct subject to the employer's control."[134] Conversely, "[a]n employee's act is not within the scope of employment when it occurs within an independent course of conduct not intended by the employee to serve any purpose of the employer."[135]

Users badged as administrators are likely agents of the site when they are conducting their administrative duties.[136] The site owners (or perhaps the community) select these users to act on their behalf, enforcing the policies they have formulated, and the badged users agree so to act. It is irrelevant that badged administrators are almost all volunteers, since "the fact that work is performed gratuitously does not relieve a principal of liability."[137] As a result, at least when badged

---

[129] *See, e.g.*, Grown Up Geek, *supra* note 84 (describing the "Hall Monitor/Peace Keeper" badge and the "Page and Code Wrangler" badge).

[130] Ken S. Myers, *Wikimmunity: Fitting the Communications Decency Act to Wikipedia*, 20 HARV. J.L. & TECH. 163, 188 (2006).

[131] *See id.* at 190 (using agency principles to distinguish Wikipedians with special editing powers from mere users of other sites); *id.* at 190–191 (using agency law to examine whether Wikipedia could argue acts were beyond the scope of an administrator's duties).

[132] RESTATEMENT (THIRD) OF AGENCY § 1.01 (2006).

[133] *Id.* § 7.07(3)(a).

[134] *Id.* § 7.07(1)–(2).

[135] *Id.* § 7.07(2).

[136] *See* Myers, *supra* note 130, at 190–91 ("Wikipedians with sysop [administrative] powers are thus more analogous to matchmaker.com and Yahoo! employees, who run the matchmaker.com and Yahoo! Profile services, than to the users who merely contribute profiles to those services." *Id.* at 190.).

[137] RESTATEMENT (THIRD) OF AGENCY § 7.07(3)(b).

administrative users are acting within the scope of their employment, for purposes of § 230, the information they provide is provided not by another information content provider, but by the interactive computer service provider itself. Under agency principles, therefore, the site receives no immunity.[138]

The issue then is what is considered the scope of employment of the badged administrative user. A site's owner could likely tolerate liability for the user's administrative acts, since in most cases administrative actions would not result in any liability. A site's owner is protected against lawsuits based on her "exercise of a publisher's traditional editorial functions — such as deciding whether to publish, withdraw, postpone or alter content."[139] The owner would be protected against liability for agents performing the same function. There would be potential liability for certain limited acts, such as a user's deletion of words in a post to make it defamatory,[140] but the owner would likely be willing to bear that limited risk as a fairly minimal price to pay for having that user's services.

It would be more harmful if the scope included the user's non-administrative posts. Ken Myers argues in regard to Wikipedia users with administrative authority ("sysops") that "[g]enerally, 'scope' is interpreted sufficiently broadly for a sysop's actions to be attributable to Wikipedia even though they *could* be performed by a non-sysop."[141] Therefore, a sysop is within the scope of his employment when "browsing, reviewing, and editing as any other registered or even unregistered user might," Myers suggests.[142]

This conclusion may make some practical sense in the world of Wikipedia. Wikipedia is a site where, by design, "[a]nyone with internet access can write and make changes to . . . articles."[143] The line between administrators and users is purposefully blurred, with "[t]heoretically all editors and users [being] treated equally with no

---

[138] *See* 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, 507 (2002) (noting that in one case "[b]oth the parties and the court seemed to realize that § 230 did not immunize AOL from liability if the defamation action was based on statements made by AOL's employees").

[139] Zeran v. Am. Online, Inc., 129 F.3d 327, 330 (4th Cir. 1997); *see also* Green v. Am. Online, 318 F.3d 465, 471 (3d Cir. 2003) (noting that "monitoring, screening, and deletion of content" are "actions quintessentially related to a publisher's role").

[140] *See* Citizen Media Law Project, Online Activities Not Covered by Section 230, http://www.citmedialaw.org/legal-guide/online-activities-not-covered-section-230 (last visited Jan. 9, 2010).

[141] Myers, *supra* note 130, at 191.

[142] *Id.*

[143] Wikipedia, Wikipedia:About, http://en.wikipedia.org/wiki/Wikipedia:About (last visited Jan. 9, 2010).

'power structure.'"[144] Everyone is working on the same text; writing and editing are often two sides of the same coin. With the roles of administrator, editor, and writer so closely intertwined, it might be hard to distinguish when the user is acting as a sysop and when he is just acting as himself, and therefore it might be more difficult to determine the scope of employment.

In contrast, the difference is clearer in other contexts. Consider the "Rescue Rangers" of the liberal political group blog *Daily Kos*, who are selected from among users who volunteer. The users look among the various posts written on a given day and pick out ones that are well written and informative but have not received very much attention.[145] This list of rescued posts is published each day in a prominent position on the site's front page, with the names of that day's Rangers listed with it. This listing of the Rangers' names is, in a very minimal way, a sort of badge, and the "rescuing" is an administrative activity.[146] The Rangers are usually active posters on the site. The roles of administrator and contributor are far easier to distinguish in this example than in the case of Wikipedia's sysops.

Courts should interpret the word "entity" and appropriate agency principles to avoid imposing liability for posts by the Rangers and other badged administrative users, at least in cases in which the line between editing and writing is easier to draw than in the context of Wikipedia's sysops. Limiting liability in this way fits with the general trend in defamation law — the area of law from which most of the claims against site owners are likely to come.[147] In the defamation law context, an employer is not liable for defamation "committed for personal motives unrelated to the furtherance of the employer's business."[148] Similarly, it would seem that a statement made by a badged administrative user in his "workplace" — whether that is a blog, message board, or wiki — would not expose a site's owner to vicarious liability unless it was "made in relation to a matter about which the employee's duties required him to act."[149] Websites could therefore

---

[144] *Id.*

[145] Posting of Unitary Moonbat to Daily Kos, http://www.dailykos.com/story/2007/6/17/205017/977 (June 17, 2007, 18:13) (describing the origin, selection, and role of the Rescue Rangers).

[146] As discussed above, if the Rangers rescued a tortious post, the site would not be exposed to liability because a decision to place the post in a prominent position is a core publishing function and therefore protected by § 230.

[147] *See* David S. Ardia, *Free Speech Savior or Shield for Scoundrels: An Empirical Study of Intermediary Immunity Under Section 230 of the Communications Decency Act*, 43 LOY. L.A. L. REV. (forthcoming 2010); *see also* Barnes v. Yahoo!, Inc., 570 F.3d 1096, 1101 (9th Cir. 2009) ("The cause of action most frequently associated with the cases on section 230 is defamation.").

[148] 1 SACK, *supra* note 90, § 2.10.2, at 2-150 (quoting Seymour v. N.Y. State Elec. & Gas, 627 N.Y.S.2d 466, 468 (App. Div. 1995)) (internal quotation marks omitted).

[149] Henderson v. Walled Lake Consol. Sch., 469 F.3d 479, 494 (6th Cir. 2006).

help themselves by clearly limiting each badged administrative user's duties.

C. Immunizing Badges and the Purposes of § 230

Interpreting the immunity provision broadly in regard to badged administrative and notable users fits with both purposes of § 230. First, it encourages editing and self-policing, albeit in a slightly different form than Congress initially intended. As discussed above, Congress feared that large internet service providers, such as CompuServe or AOL, would refuse to edit posts on discussion groups because they would be liable if and when they missed something. In the Web 2.0 world, administrator badges give a site more eyes to find objectionable content and edit, move, or delete it. If liability were imposed against sites, either for a perceived endorsement or on an agency basis, sites would be unlikely to badge these users. The result would be exactly what Congress feared — a "backward" world where "computer Good Samaritans . . . who take[] steps to screen indecency and offensive material for their customers" (and who take steps to make good content more clearly available) face liability.[150]

Second, construing the immunity provision broadly to cover badged users promotes the development of free speech and of e-commerce online, though again perhaps in a slightly different way than Congress originally intended. Badges indicating user quality help users discover for themselves what content is worth reading and unobjectionable.[151] With regard to badged administrative users, as discussed above, they are some of the most involved community members on any given site. Yet if liability were imposed when a badged administrative user posted information, site owners would be forced to choose between accepting such liability, limiting those users' ability to post — either by requiring their posts to be prescreened or by preventing them from posting at all, at least under their usual usernames — or not badging in the first place. Any one of these options would severely hamper free speech online. Alternatively (and more likely), these experienced users would choose not to accept a badge with such restrictions, depriving the site of its best potential editors and hindering Congress's goal of promoting self-editing.

Opponents of this argument might contend that, even if liability were imposed, sites would still badge users. Some sites might still do

---

[150] 141 CONG. REC. 22,045 (1995) (statement of Rep. Cox).

[151] *Cf.* Carafano v. Metrosplash.com, Inc., 339 F.3d 1119, 1124–25 (9th Cir. 2003) ("Without standardized, easily encoded answers, [the site] might not be able to offer these services and certainly not to the same degree. Arguably, this promotes the expressed Congressional policy 'to promote the continued development of the Internet and other interactive computer services.'" *Id.* at 1125 (quoting 47 U.S.C. § 230(b)(1) (2006))).

so, of course, taking on liability for the enhanced prestige of having more easily identifiable good content and editing. As the court in *Stratton Oakmont* pointed out with regard to Prodigy's editing, the market may "compensate a [website] for its increased control and resulting increased exposure."[152] But inevitably, many sites faced with liability for the acts of their badged users would choose to not allow the users themselves to award badges for quality, instead having only the operator recognize such users or having no recognition at all. Similarly, these sites would refuse to select volunteer administrators. Without badges, at best good posts would be harder to find. Without administrator badges in particular, the larger message boards and group blogs would be virtually unmanageable.[153] Opponents of granting immunity for badging could contend that sites could still appoint administrators without badging them, but this argument overlooks the fact that community control works best if the users doing the administrating are known to be prominent, respected community members. Administrators whose identities are concealed would not have the same respect. In 1995, Congressman Christopher Cox expressed his fear that there was "just too much going on on the Internet" for government regulators to monitor and control it.[154] Today, there is vastly more going on, far too much for even site operators to control; they need the help of volunteers.

IV. CONCLUSION

Badges are an important tool to help users find their way in a Web 2.0 world. They help people find out which users are most likely to give them useful information and allow site owners to empower community members to help retain control over an ever-growing flood of information. Section 230 has been a great help so far in both generally allowing Web 2.0 sites to exist and specifically encouraging site owners to utilize badged users. Courts should continue to interpret § 230 broadly in this context, in order to respect Congress's joint goals in enacting it and to make the web a safer, more innovative, and more useful place.

---

[152] Stratton Oakmont, Inc. v. Prodigy Servs. Co., No. 031063/94, 1995 WL 323710, at *5 (N.Y. Sup. Ct. May 24, 1995).

[153] *Cf.* DiMeo v. Max, 433 F. Supp. 2d 523, 528 (E.D. Pa. 2006) ("Absent [§ 230] protection interactive computer services would essentially have two choices: (1) employ an army of highly trained monitors to patrol (in real time) each chatroom, message board, and blog to screen any message that one could label defamatory, or (2) simply avoid such a massive headache and shut down these fora. Either option would profoundly chill Internet speech.").

[154] 141 CONG. REC. 22,045 (1995) (statement of Rep. Cox).