THE OPTIMAL LIABILITY SYSTEM FOR ONLINE SERVICE PROVIDERS: HOW *ZERAN V. AMERICA ONLINE* GOT IT RIGHT AND WEB 2.0 PROVES IT

By Cecilia Ziniti

> *Should businesses be liable for the grafitti [sic] on their walls? No, it's the one who put it there who should be in trouble.*
>
> —Comment to blog entry on the scope of CDA immunity.[1]

> *It would be altogether unreasonable to demand so near an approach to omniscience . . . . [T]he bookseller's burden would become the public's burden, for by restricting him the public's access to reading matter would be restricted.*
>
> —The court in Smith v. California, an offline content distributor liability case.[2]

I. INTRODUCTION

Much has changed since 1997, when the Fourth Circuit in *Zeran v. America Online*[3] became the first appellate court to interpret § 230 of the Communications Decency Act ("CDA"). Section 230 immunizes online service providers from liability for third-party content. Evaluating § 230 and the case law interpreting it reveals a remarkably good legal framework that has truly fostered the last ten years' development of the web.

Part II of this Note reviews the statutory background of § 230, outlines the critical *Zeran* holdings on the CDA, and reviews post-*Zeran* developments in the online world. Against that background, Part III considers the liability of online providers for third-party content generally and discusses potential alternatives to § 230's wide grant of immunity under *Zeran*. It also highlights problems with such alternatives. Part IV concludes with an explanation of how the post-*Zeran* cases have created a liability scheme constitutionally, practically, and socially preferable to its alternatives—especially as applied to the new landscape of online services.

---

1. Posting of "Daniel" to TechDirt Blog, There's A Good Reason Why Online Sites Shouldn't Be Liable For The Actions Of Its Users, http://www.techdirt.com/article.php?sid=20060908/163844#c19 (Sept. 8, 2006, 18:10 PST) (commenting on § 230 of the Communications Decency Act).

2. Smith v. California, 361 U.S. 147, 153 (1959) (internal quotations and citations omitted).

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

II. STATUTORY BACKGROUND

Passed as an amendment to the Telecommunications Act of 1996,[4] § 230 of the Communications Decency Act[5] ("CDA") creates a safe harbor for online service providers—section 230(c)(1)—that shields them from liability for their users' actions and related content.[6] Section 230(c)(1) directs that "[n]o 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."[7] With that provision, Congress explicitly departed from common law defamation jurisprudence. That jurisprudence had determined an actor's liability for third-party content based on the level of control the actor exercised over it.[8] At common law, that a party exerted or could exert more control over third-party content led to the application of stricter liability standards for it.[9]

Specifically, in passing § 230, Congress sought to overrule a New York case, *Stratton Oakmont, Inc. v. Prodigy Services Co.*,[10] in which the court held that an online service provider, Prodigy, acted as a publisher when it screened some areas of its site to make the site more family-friendly.[11] Under common law defamation principles, the court held that, as a publisher, Prodigy was fully responsible for liability arising from third-party generated message board postings—despite Prodigy's lack of contribution to, notice of, or knowledge of the postings' unlawful nature.[12] Prodigy's good-faith efforts to monitor its site thus resulted in increased liability under common law principles. Legislators recognized the unfair-

4. Telecommunications Act of 1996, Pub. L. No. 104-104, 110 Stat. 56 (codified as amended in scatted sections of 47 U.S.C.). The Supreme Court held that §§ 223(a) and 223(d) of the Communications Decency Act, aimed at restricting access to pornographic material on the Internet, violated the First Amendment. Reno v. ACLU, 521 U.S. 844 (1997).

5. 47 U.S.C. § 230 (2000).

6. Carafano v. Metrosplash.com, Inc., 339 F.3d 1119, 1123 (9th Cir. 2003) ("[R]eviewing courts have treated § 230(c) immunity as quite robust.").

7. 47 U.S.C. § 230(c)(1) (2000).

8. *See* Paul Ehrlich, Note, *Regulating Conduct on the Internet: Communications Decency Act § 230*, 17 BERKELEY TECH. L.J. 401, 402-03 (2002) (discussing "The Pre-CDA Landscape").

9. *Id.*

10. No. 31063/94, 1995 N.Y. Misc. LEXIS 229 (N.Y. Sup. Ct. May 24, 1995).

11. *Id.* at *10-11. H.R. REP. NO. 104-458, at 194 (1996) (Conf. Rep.), *reprinted in* 1996 U.S.C.C.A.N. 10, 207-08 ("One of the specific purposes of [section 230] is to overrule *Stratton Oakmont v. Prodigy* and any other similar decisions which have treated such providers and users as publishers or speakers of content that is not their own because they have restricted access to objectionable material.").

12. *See Stratton Oakmont*, 1995 N.Y. Misc. LEXIS 229, at *6-7.

ness of the *Stratton Oakmont* result—i.e., that the huge volume of web content distinguishes it from traditional media and makes application of traditional liability schemes unfair.[13]

A. Early Judicial Interpretation and the Zeran Regime

Almost uniformly, courts have interpreted § 230's safe harbor broadly.[14] Under § 230(c)(1), online service providers, including website operators, have enjoyed immunity from primary and secondary liability for a wide variety of claims including defamation, employment torts, negligent misrepresentation, cyber-stalking, and breach of contract.[15] The safe harbor provides immunity from being "treated as [a] publisher,"[16] a phraseology courts have given expansive meaning. Courts' broad construction likely stems from the statute's stated aims: "to promote the continued development of the Internet" and "preserve the vibrant and competitive free market" online.[17]

B. The *Zeran* Case

The Fourth Circuit's *Zeran v. America Online*[18] established the foundation for broad interpretation of § 230.[19]

---

13. *See* 141 CONG. REC. H8471 (daily ed. Aug. 4, 1995) (statement of Rep. Goodlatte) ("There is no way that any of those entities, like Prodigy, can take the responsibility to edit out information that is going to be coming in to them from all manner of sources onto their bulletin board . . . . [T]o have that imposition imposed on them is wrong.").

14. *Carafano*, 339 F.3d at 1122-23 (citing Batzel v. Smith, 333 F.3d 1018, 1026-27 (9th Cir. 2003)). *See also* Chi. Lawyers' Comm. for Civ. Rights Under the Law v. Craigslist, 461 F. Supp. 2d 681 (N.D. Ill. Nov. 14, 2006) ("Virtually all subsequent courts that have construed Section 230(c)(1) followed *Zeran*, and several have concluded that Section 230(c)(1) offers [interactive computer service]s a "broad," "robust" immunity.") (collecting cases). *But see* Barrett v. Rosenthal, 114 Cal. App. 4th 1379, 1402-08 (2004) (citing criticism of *Zeran*'s broad interpretation and holding immunity not to apply), *rev'd*, Barrett v. Rosenthal, 40 Cal. 4th 33 (2006).

15. There was for short while an open question as to whether, given the inclusion of terms traditionally found in defamation jurisprudence (i.e., words like 'publisher' and 'speaker'), section 230 applied to any causes of action besides defamation. *See* Schneider v. Amazon.com, 108 Wash. App. 454, 464-465 & n.25 (2001). The issue has since been settled in the affirmative—so much so that a leading commentator concludes that for plaintiffs to even make the argument that 230 immunizes providers only with respect to defamation claims is "lame and futile." *See* Posting of Eric Goldman to Technology & Marketing Law Blog, Ninth Circuit Screws Up 47 USC 230—Fair Housing Council v. Roommates.com, http://blog.ericgoldman.org/archives/2007/05/ninth_circuit_s.htm (May 15, 2007 11:59).

16. 47 U.S.C. § 230(c)(1) (2000).

17. 47 U.S.C. § 230(b)(1)-(2) (2000).

18. Zeran v. Am. Online, Inc., 129 F.3d 327 (4th Cir. 1997).

1. Zeran*'s Framework for Immunity*

The court in *Zeran* held defendant America Online ("AOL") was immune under § 230.[20] The plaintiff claimed that after a third-party defamed him by posting messages on an AOL message board, AOL exacerbated his injuries by failing to timely remove the content upon notice.[21] Though it did not characterize it exactly as such, the *Zeran* court laid out what in effect functions as a three-part test for § 230(c)(1) immunity.[22] The defendant service provider must demonstrate: (1) that it was acting as a user or provider of an "interactive computer service,"[23] and (2) that holding it liable in the manner the plaintiff seeks would treat the defendant "as the publisher or speaker" of information furnished "by another information content provider";[24] and (3) that the defendant itself was not the "information content provider" of the content at issue.[25] In *Zeran*, the plaintiff conceded the third part of the test.[26]

2. Zeran*'s Controversial Holdings*

Beyond the relatively straightforward framework culled from the statute, the *Zeran* court made additional judgments about the scope of service provider immunity[27] that have generated controversy among commentators and subsequent courts.[28]

The court in *Zeran* held that § 230 precluded not just strict liability as a publisher, as in *Stratton Oakmont*.[29] Rather, said the court, it also pre-

---

19. According to a Lexis search on March 9, 2008, more than 60 federal cases across every circuit and 25 state court opinions across eleven states cite *Zeran*.

20. *Zeran*, 129 F.3d at 328, 335.

21. *See id.* at 330, 331.

22. *Id.* at 330.

23. *Id.* at 330 (citing 47 U.S.C. § 230(c)(1)). The CDA defines "interactive computer service" as "any information service, system, or access software provider that provides or enables computer access by multiple users." 47 U.S.C. § 230(f)(2).

24. *Zeran*, 129 F.3d at 330 (citing 47 U.S.C. § 230(c)(1)). The CDA defines an "information content provider" as any person or entity "responsible, in whole or in part, for the creation or development" of the information at issue. 47 U.S.C. § 230(f)(3).

25. *Zeran*, 129 F.3d at 330.

26. *Id.* at 330 n.2 (noting that the parties agreed that AOL qualified as an "interactive computer service" because an unknown third party was the "information content provider" of the information at issue).

27. *Id.* at 330-34.

28. *See* Barrett v. Rosenthal, 114 Cal. App. 4th 1379, 1393-95 (2004) (calling *Zeran*'s characterization of § 230 "misleading" and collecting scholarly and courts' criticism of it).

29. *Compare Stratton Oakmont*, at *6 (contrasting publisher and distributor liability with respect to knowledge and fault requirements) *with Zeran*, 129 F.3d at 332 ("[D]istributors are considered to be publishers for purposes of defamation law.").

cluded the application to website operators of intermediate liability for *distributors*,[30] a category of defendants that, before § 230, had faced liability upon knowledge of or negligence with respect to offending content they distributed.[31] Instead, it held distributors were a subset of publishers and were thus immunized by § 230.[32] Under this reading, providers maintain § 230 immunity even if they choose not to take action after learning of potentially illegal content on their sites.[33] Thus, the *Zeran* court implied that § 230 immunity applies not just to publication-related claims, such as defamation, but to *all* claims not explicitly excluded in the statute (criminal, IP and communication privacy claims).[34]

Furthermore, the *Zeran* court reasoned that precluding distributor liability was the only holding consistent with Congress's intent.[35] It found that intent "not difficult to discern," especially in light of express Congressional findings in § 230 that it was "'the policy of the United States . . . 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*.'"[36] Thus, said the court, Congress necessarily sought to avoid "the specter of tort liability in an area of such prolific speech [the Internet]" and the "obvious chilling effect" that a holding otherwise—i.e., that § 230 only immunized traditional activities of publishers—would entail.[37]

---

30. *Zeran*, 129 F.3d at 332-33.

31. *See, e.g.*, Cubby, Inc. v. Compuserve, Inc., 776 F. Supp. 135, 139 (S.D.N.Y. 1991) ("With respect to entities such as news vendors, book stores, and libraries, however, 'New York courts have long held that vendors and distributors of defamatory publications are not liable if they neither know nor have reason to know of the defamation.'").

32. *Zeran*, 129 F.3d at 332.

33. *See* Universal Commc'n Sys. v. Lycos, Inc., 478 F.3d 413, 420 (1st Cir. 2007) (explaining that under *Zeran*, "[i]t is, by now, well established that notice of the unlawful nature of the information provided is not enough to make it the service provider's own speech. . . . Section 230 immunity applies even after notice.")

34. *Zeran*, 129 F.3d at 330 ("By its plain language, § 230 creates a federal immunity to any cause of action that would make service providers liable for information originating with a third-party user of the service."). Subsequent courts have read *Zeran* this way. *See* Christopher Butler, *Plotting the Return of an Ancient Tort to Cyberspace: Towards a New Federal Standard of Responsibility for Defamation for Internet Service Providers*, 6 MICH. TELECOMM. TECH. L. REV. 247, 248, 254-56 (2000) (explaining how the § 230 regime that developed under *Zeran* became a "prohibition against virtually all liability" rather than classification of ISP liability as that of common law distributors), *available at* http://www.mttlr.org/volsix/Butler.html.

35. *Zeran*, 129 F.3d at 330-33.

36. *Id*. at 330 (citing § 230(b)(1)) (emphasis in original).

37. *Zeran*, 129 F.3d at 331.

*3. Post-*Zeran

Soon after *Zeran*, the court in *Blumenthal v. Drudge*[38] applied *Zeran* to a case that highlighted—or perhaps obfuscated—the distinction under § 230 between a (non-immune) content provider and an (immune) interactive service provider.[39] The defendant in *Blumenthal*, AOL, had more control over the content in question than it had in *Zeran* because it paid for, promoted, and retained editorial control over the allegedly defamatory content.[40] Nevertheless, the court, citing *Zeran*, held AOL immune under § 230, regardless of whether AOL might under common law have qualified as a content distributor or even as a publisher.[41] In so doing, the court echoed *Zeran*'s interpretation of § 230, i.e., that Congress did not intend § 230 to at all distinguish between publishers' and distributors' qualification for immunity.[42] The court agreed with *Zeran*'s reasoning that Congress's policy choice in passing § 230 required immunity for AOL. Congress, said the court, had established a "tacit *quid pro quo*" of offering interactive service providers broad immunity in exchange for their efforts to police themselves.[43]

Scholars have criticized the reasoning in *Zeran* and its progeny and their expansion of § 230's safe harbor.[44] Critics deny that Congress intended to extend immunity to distributors, and they take issue with *Zeran*'s contention that Congress's primary objective in passing § 230 was avoiding tort liability's chilling effects on free speech.[45] In contrast, inter-

38. 992 F. Supp. 44 (D.D.C. 1998).

39. *See* 47 U.S.C. §§ 230(c)(1), (f)(2)-(3) (2000).

40. *Blumenthal*, 992 F. Supp at 50-51.

41. *Id.* at 53.

42. *Id.* at 52-53.

43. *Id.* at 52.

44. *See* Barrett v. Rosenthal, 114 Cal. App. 4th 1379, 1395 (2004) ("The view of most scholars who have addressed the issue is that *Zeran*'s analysis of section 230 is flawed, in that the court ascribed to Congress an intent to create a far broader immunity than that body actually had in mind or is necessary to achieve its purposes.") (collecting sources).

45. *See, e.g.*, Jennifer C. Chang, *In Search of Fair Housing in Cyberspace: The Implications of the Communications Decency Act for Fair Housing on the Internet*, 55 STAN. L. REV. 969, 995-96 & n.111 (2002) (criticizing *Zeran*'s "flawed logic"); Butler, *supra* note 34, at 253-54 (2000) (arguing that, by eliminating the common law's publisher/distributor distinction, the *Zeran* court incorrectly read § 230 more broadly than Congress intended); Ian C. Ballon, *Zeran v. AOL: Why the Fourth Circuit Is Wrong*, J. INTERNET L. (Mar. 1998), *available at* http://library.findlaw.com/1999/Feb/2/127916.html ("While the elimination of all third party liability for defamation would be generally consistent with the goal of promoting unfettered free speech online, it is incon-

net companies at the time and since, have lauded *Zeran*, with AOL's counsel predicting that the case "would stand the test of time" because it was "well written and well-reasoned."[46] Fairly assessing *Zeran* as applied today, though, requires a review of how the Internet today differs from when *Zeran* was decided.

C. Changes Since § 230's Passage and the *Zeran* Decision

1. Tremendous Growth

Since the passage of § 230 and the *Zeran* decision, the Internet has changed tremendously, as has American engagement with it. Over 70% of Americans are online, up from under 30%.[47] The term 'blog' emerged, and the number of them increased from essentially none to over 70 million.[48] Search engine Google went from a nifty Ph.D. project[49] to a multinational corporation with a market capitalization of over $200 billion.[50] Online encyclopedia Wikipedia debuted and grew to include entries on over two million topics.[51] Overall, the web grew to over 600 billion pages—over

---

sistent with the objective of encouraging . . . self-regulation [by online service providers].").

46. *See* In Brief, *U.S. Supreme Court Monday Let Stand Lower Court Decision*, COMMC'NS DAILY (Warren Publ'g), June 23, 1998 (quoting George Vradenburg, then general counsel for *Zeran* defendant AOL). *See also* Brief of Amici Curiae Amazon.com, Inc., et. al., *Barrett v. Rosenthal*, 40 Cal. 4th 33 (2006) (No. S122953), *available at* http://www.eff.org/files/filenode/Barrett_v_Rosenthal/ISP_amicus_brief.pdf (featuring internet companies like Amazon, eBay, and Google calling *Zeran* "seminal" and "well-reasoned" and calling for the court to follow it).

47. MARY MADDEN, PEW INTERNET & AMERICAN LIFE PROJECT, DATA MEMO: INTERNET PENETRATION AND IMPACT 3 (2006), *available at* http://www.pewinternet.org/pdfs/PIP_Internet_Impact.pdf.

48. Andy Carvin, *Timeline, The Life of the Blog*, NPR.ORG, Dec. 24, 2007, http://www.npr.org/templates/story/story.php?storyId=17421022; Posting of David Sifry, to Sifry's Alerts, The State of the Live Web, April 2007, http://www.sifry.com/alerts/archives/000493.html (Apr. 5, 2007 02:02:00) ("Technorati is now tracking over 70 million weblogs, and we're seeing about 120,000 new weblogs being created worldwide each day. That's about 1.4 blogs created every second of every day.").

49. Google Milestones, http://www.google.com/intl/en/corporate/history.html (last visited Oct. 7, 2007) (showing market capitalization of Google, Inc. was over $200,000,000,000).

50. *See* Google, Inc. (GOOG), Yahoo! Finance, http://finance.yahoo.com/q?s=GOOG (last visited Oct. 27, 2007).

51. Wikipedia:About, http://en.wikipedia.org/wiki/Wikipedia:About (last visited Sept. 23, 2007).

100 pages per person on earth.[52] Total search engine traffic grew by orders of magnitude since *Zeran*, to over 250 million searches per day today.[53]

2. The Rise of Web 2.0

Moreover, the way people interact with the web has changed. At the time of *Zeran*, Web users observed, found, and exchanged content passively, e.g., by reading the *Washington Post* online, browsing the web using static directories like the original Yahoo!,[54] and privately, e.g., by emailing or engaging in person-to-person instant messages. Users now play a much more active role in creating and generating content for public or semi-public view.[55] They keep in touch not just using email, but by creating detailed, content-filled profile pages on sites like MySpace and Facebook.[56] They use systems to find, filter, and monitor the web's content via custom RSS news feeds, search-based alerts, and social networks. These developments, sometimes referred to as "Web 2.0" and social media, discussed in detail below, have developed and entered the mainstream

52. *See* Kevin Kelly, *We Are the Web*, WIRED, Aug. 20, 2005, at 96, *available at* http://www.wired.com/wired/archive/13.08/tech.html.

53. Press Release, Nielsen//NetRatings, Nielsen//NetRatings Announces August U.S. Search Share Rankings (Sept. 19, 2007), http://www.nielsen-netratings.com/pr/pr_070919.pdf (listing that total web searches per day in August 2007 was 250 million). *See generally* JOHN BATTELLE, THE SEARCH: HOW GOOGLE AND ITS RIVALS REWROTE THE RULES OF BUSINESS AND TRANSFORMED OUR CULTURE, 39-63, 123-43 (2006).

54. *See* Yahoo!, http://web.archive.org/web/19971022190737/http://www11.yahoo.com/ (showing Yahoo! at the time of *Zeran*) (last visited Feb. 8, 2008); Yahoo! Directory, http://dir.yahoo.com/ (showing the Yahoo! directory today) (last visited Feb. 8, 2008).

55. *See* Lev Grossman, *Time's Person of the Year: You*, TIME, Dec. 13, 2006—Jan. 1, 2007, at 38, 40-41; ELECTRONIC FRONTIER FOUNDATION, ET. AL., FAIR USE PRINCIPLES FOR USER GENERATED VIDEO CONTENT 1 (2007), http://www.eff.org/files/UGC_Fair_Use_Best_Practices_0.pdf (2007) ("By providing a home for 'user-generated content' (UGC) on the Internet, these services enable creators to reach a global audience . . . . The result has been an explosion of creativity by ordinary people, who have enthusiastically embraced the opportunities created by these new technologies to express themselves in a remarkable variety of ways."); James Grimmelmann, *Don't Censor Search*, 117 YALE L.J. POCKET PART 49, 51 (2007), http://thepocketpart.org/2007/09/08/grimmelmann.html (arguing that advances in search technology "can help individuals move from being passive consumers of information to active seekers for it" and "catalyze[] a virtuous cycle of creativity.").

56. *See* Posting of Aidan Henry to Mapping the Web, Is Facebook Replacing Email?, http://www.mappingtheweb.com/2007/07/11/facebook-email/ (Jul. 11, 2007) (pointing out that younger internet users tend to use Facebook's open message system rather than email); Alice Mathias, *The Fakebook Generation*, N.Y. TIMES, Oct. 6, 2007, at A19 (quoting one Facebook user explaining that she has "always thought of Facebook as online community theater. . . .").

since *Zeran* defined the scope of § 230 immunity. Loosely defined, Web 2.0 embodies interactive service providers that leverage users' collective intelligence and make the web, not the PC, "the platform that matters."[57]

Scholars and courts alike have recognized the vast social utility the Internet and search engines provide under these new interaction models.[58] Mark Lemley points to the web's positive externalities.[59] He notes that internet services "do not and cannot reasonably expect to capture anything like the full social value of the uses that pass through their system."[60] The website and community Craigslist, for example, employs fewer than 30 people and offers most of its services for free.[61] Yet its users are enormously loyal,[62] and the site attracts over 8 billion page views and 35 million users per month, making it one of the top sites on the web.[63] By leaving a tremendous amount of revenue untapped, the site generates positive externalities for its users.[64] Moreover, social value theory applies with particular force online. Anyone with access to a public library can access the Internet and keep a blog. Low barriers to entry give the masses unprecedented power to access, create, and publish.[65]

---

57. Tim O'Reilly, *Not 2.0?*, O'REILLY RADAR, Aug. 5, 2005, http://radar.oreilly.com/archives/2005/08/not_20.html ("The net has replaced the PC as the platform that matters, just as the PC replaced the mainframe and minicomputer.").

58. *See, e.g.*, Am. Library Ass'n v. United States, 201 F. Supp. 2d 401, 405 (E.D. Pa. May 31, 2002) ("the beneficial effect of the Internet in expanding the amount of information available to its users is self-evident . . . ."), *rev'd*, 539 U.S. 194 (2003); BATTELLE, *supra* note 53, at 7-9 (expressing wonder at the power of search engines to transform our daily lives); YOCHAI BENKLER, THE WEALTH OF NETWORKS 1-91 (2006) (extolling the power of the Internet and the "networked information economy" to enrich society), *available at* http://www.benkler.org/Benkler_Wealth_Of_Networks.pdf; Frank Pasquale, *Copyright in an Era of Information Overload: Toward the Privileging of Categorizers*, 60 VAND. L. REV. 135 (2007) (advocating special fair use treatment for search engines because of the social utility they provide in reducing search costs).

59. Mark A. Lemley, *Rationalizing Internet Safe Harbors* 15 (Stanford Public Law Working Paper, No. 979836, 2007), *available at* http://ssrn.com/abstract=979836.

60. *Id.*

61. *See* Craigslist Fact Sheet, http://www.craigslist.org/about/factsheet.html (last visited Oct. 28, 2007).

62. Anita Hamilton, *Find it on Craigslist*, TIME, Mar. 3, 2003, at 76.

63. *Id.*

64. Andrew Ross Sorkin, *Craigslist Meets the Capitalists*, N.Y. TIMES, Dec. 8, 2006 (Dealbook blog) http://dealbook.blogs.nytimes.com/2006/12/08/craigslist-meets-the-capitalists/.

65. *See* Frank A. Pasquale & Oren Bracha, *Federal Search Commission? Access, Fairness and Accountability in the Law of Search* 8-9 (Univ. of Texas Law Public Law Research Paper, No. 123, 2007), *available at* http://ssrn.com/abstract=1002453.

3. Characteristics of Web 2.0 Service Providers

Web 2.0 services share certain core principles.[66] In Web 2.0, for example, online services do not simply give users access to the web and a voice online—rather, they help find, manage, and explore the data within the web to make it useful.[67] Under this model, "the value of software [in Web 2.0] is proportional to the scale and dynamism of the data it helps to manage."[68] Services like photo-sharing and community site Flickr, or Amazon.com's community ratings system, take inputs from millions of users in the form of ratings, tags, and engagement (e.g., via analyzing what and how much users click, comment on, or forward to their friends) to make the online experience better.[69] User input not only improves but indeed makes possible technologies ranging from optimal spam filtering to social networking to movie ratings systems. Start-ups like Aggregate Knowledge and Clickability have entire business models based on helping websites harness the power of—and revenue from—user communities.[70] In short, "the heart of Web 2.0 is the user . . . . The tools power it, but the people do it."[71]

Other features associated with Web 2.0 are open content and the offering of application program interfaces ("APIs") and other technical means for users to manipulate content.[72] Mashups, or programs that allow users to combine data from different sources into one tool,[73] are also new since *Zeran*. Likewise, services like Google's AdSense, which enables anyone

---

66. Tim O'Reilly, *What Is Web 2.0: Design Patterns and Business Models for the Next Generation of Software*, O'REILLY NETWORK, Sept. 30, 2005, http://www.oreillynet.com/pub/a/oreilly/tim/news/2005/09/30/what-is-web-20.html.

67. *Id.*

68. *Id.*

69. *Id.*

70. *See* About Us, http://www.clickability.com/company/About.html (last visited Feb. 23, 2008); Overview, http://www.aggregateknowledge.com/about.html (last visited Feb. 23, 2008).

71. Posting of Susan Mernit to Susan Mernit's Blog, Web 2.0—It's Not Just RSS, http://susanmernit.blogspot.com/2005/09/web-20-its-not-just-rss.html (Sept. 27, 2005).

72. *See* Kwei-Jay Lin, *Building Web 2.0*, COMPUTER, IEEE Computer Society, May 2007, at 101-02 ("Any Web-based software that lets users create and update content is arguably a Web 2.0 technology . . . . Providing friendly tools for user participation in content creation, consumption, and distribution has been the key to success (and failure) for many startups in the Web 2.0 era.").

73. Posting of Sherif Mansour to Smalls Blogger, Why Mashups = (REST + 'Traditional SOA') * Web 2.0, http://blog.sherifmansour.com/?p=187 (Dec. 5, 2007) ("A Mashup is a new service, that combines functionality or content from existing sources. These existing sources can be Web Services (through the use of API's), RSS feeds or even just other Websites (by screen-scraping.")).

with a blog to make money by hosting Google ads on it, represent the web's new "distributed" model wherein much of the activity, profitable and otherwise, happens at edge rather than in a few concentrated centers.[74]

In essence, Web 2.0 services embrace and encourage the "long tail"[75] such that the classic economic notion of the network effect[76]—that the value of a network to a given customer depends on the numbers of users of it—proves even more powerful in Web 2.0 than on the Web before it.[77] That means restricting human input to Web 2.0, even marginally, necessarily destroys value. Furthermore, as a result of the network effect, restricting user input destroys value not just linearly—i.e., by a fixed amount per user excluded—but exponentially.

4. The Legal Implications of Web 2.0

The shift to Web 2.0 has important legal implications for publishing, distributing, and creating content in cyberspace. Under pre-*Zeran* jurisprudence, even technology as innocuous as a spam filter, because it entails some review by the provider of the email filtered, could make its provider the publisher of, and therefore liable for claims arising from, email content.[78] Namely, the *Stratton Oakmont* court's conclusion that Prodigy became a publisher "by actively utilizing technology and manpower to delete notes from its computer bulletin boards" would likely require that result.[79] The same analysis would also apply to many Web 2.0 services. For example, sites that, like photo site Flickr, sort and present user-generated con-

---

74. *See* O'Reilly, *supra* note 66, at 2 ("The Web 2.0 lesson: *leverage customer-self service and algorithmic data management to reach out to the entire web, to the edges and not just the center, to the long tail and not just the head.*") (emphasis in original).

75. For a general discussion of the "long tail" concept online and offline, see CHRIS ANDERSON, THE LONG TAIL: WHY THE FUTURE OF BUSINESS IS SELLING LESS OF MORE (2006).

76. One popular way to express this notion is the so-called Metcalfe's Law: that the value of a communications network like the Internet to its users is proportional to the square of the number of users of the system. *See* Posting of Bob Metcalfe to VCMike's Blog, Metcalfe's Law Recurses Down the Long Tail of Social Networking, http://vcmike.wordpress.com/2006/08/18/metcalfe-social-networks/ (Aug. 18, 2006).

77. *See* O'Reilly, *supra* note 66, at 2 ("Network effects from user contributions are the key to market dominance in the Web 2.0 era."); *see also* Posting of Dion Hinchcliffe to Dion Hinchcliffe's Web 2.0 Blog, Hacking the Web's Network Effect, http://web2.socialcomputingmagazine.com/hackingwebnetworkeffect.htm (Oct. 17, 2005) ("Network effects are a primarily [sic] reason that the Web is such a vibrant and exciting place today.").

78. *See Stratton Oakmont*, 1995 N.Y. Misc. LEXIS 229 at *10.

79. *See id. But see* Douglas B. Luffman, *Defamation Liability For On-Line Services: The Sky Is Not Falling*, 65 GEO. WASH. L. REV. 1071 (1997) (arguing that *Stratton Oakmont* would not require such a result for most internet services).

tent according to user-defined tags also "actively utilize[e] technology" to manipulate content.[80] Staying with the Flickr example: the site features user-submitted photos on its homepage based on user-added "tags" such that, for instance, on Valentine's Day, photos tagged with the word "love" automatically rotate out on the site's primary landing page.[81] A court could logically conclude, then, that Flickr therefore exercises "editorial control" over the photo's content because it, or at least its technology, must decide which tags to feature and then "reviews" the photos to categorize and channel them.

Web 2.0 icon Wikipedia might be a publisher under *Stratton Oakmont* too, especially in light of the "impression of institutional reliability and veracity" it affords and the fact that it organizes content by subject and suggests areas for user input.[82] Publisher liability as understood at common law would lead to input restrictions that would, because of the network effects that enable Wikipedia,[83] destroy significant value. Such a standard could, for example, limit entries on categories like Gattinara wine[84] or orthogonal frequency-division multiplexing[85]—areas in which few people have expertise and which offline encyclopedias exclude. These kinds of entries make Wikipedia more useful, so removing them would prove costly.

III. DEFINING THE OPTIMAL LIABILITY SYSTEM FOR THIS NEW WORLD ONLINE

This Part argues that, especially as applied to Web 2.0, the *Zeran* regime—though not costless—proves superior to alternatives. Section III.A provides an overview of the spectrum of liability schemes. Section III.B begins an in-depth examination of alternatives, starting with a reversion to common law jurisprudence. Section III.C explores the possibility of im-

---

80. *See Stratton Oakmont*, 1995 N.Y. Misc. LEXIS 229 at *10.

81. For an example of a page comprised of images collected based on user-defined tags, see Flickr: Photos Tagged with Love, http://www.flickr.com/photos/tags/love/clusters/ (last visited Feb. 24, 2008).

82. *See* Anita Ramasastry, *Is an Online Encyclopedia, Such as Wikipedia, Immune From Libel Suits? Under Current Law, the Answer Is Most Likely Yes, But that Law Should Change*, FINDLAW'S WRIT, Dec. 12, 2005, http://writ.news.findlaw.com/ramasastry/20051212.html.

83. *See* Wikipedia, Network Effect, http://en.wikipedia.org/wiki/Network_effect (last modified Feb. 14, 2008) ("Wikipedia itself depends on positive network effects.").

84. Wikipedia, Gattinara Wine, http://en.wikipedia.org/wiki/Gattinara_(wine) (last modified Oct. 8, 2007).

85. Wikipedia, Orthogonal Frequency-Division Multiplexing, http://en.wikipedia.org/wiki/Orthogonal_frequency-division_multiplexing (last modified Feb. 6, 2008).

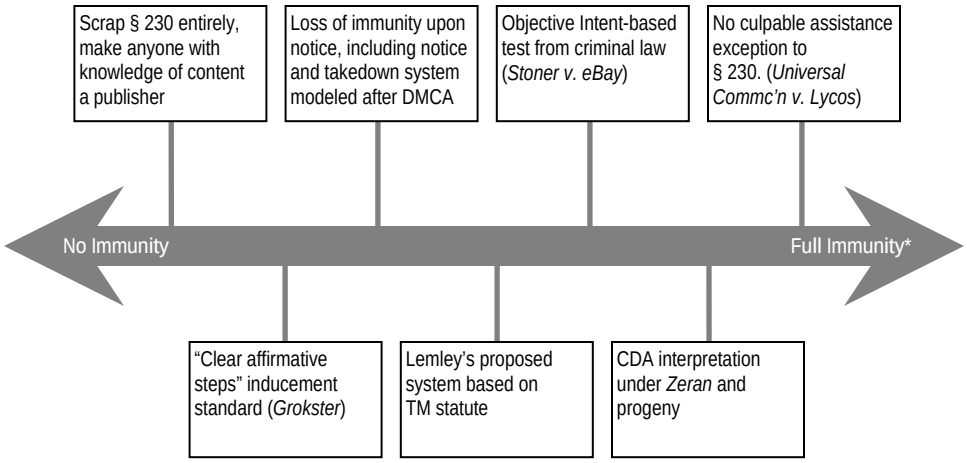
posing liability upon knowledge or notice. Section III.D considers intent-based standards, like the "affirmative steps" approach the Supreme Court took in *MGM v. Grokster*. Section III.E briefly considers other possibilities. Section III.F then looks at the cost and benefits of *Zeran* against the background of the alternatives.

This Part concludes that increased liability on interactive service providers would have negative externalities, be constitutionally problematic, and put the brakes on Web 2.0. Internet services currently immune under *Zeran* and its progeny would lose immunity under alternate schemes, thus facing draining legal battles to which they would react in predictable ways—diminishing the value and promise of Web 2.0. Alternatives to *Zeran* would inhibit providers' ability to provide useful, entertaining, and socially beneficial online experiences based on user-generated content. Furthermore, depending on how they are implemented, more rigorous liability frameworks would likely impermissibly restrict free speech.

A. The Liability Spectrum

Decreases in value might prove warranted and necessary, but in crafting a legal liability system for the web, courts and policymakers should account for them. Thus the challenge of Web 2.0 for the law: How can the law assign liability for content, when Web 2.0 providers encourage the development of the content on the front end, redistribute it on the back end, manipulating the content all along the way? How much protection should the law afford Web 2.0 companies given their tremendous value to users, society, and shareholders? The spectrum of possible responses ranges from traditional common law defamation jurisprudence, which offers no immunity at all, at one extreme, to full immunity regardless of the service provider's editing, encouragement, knowledge, or intent with respect to user-created content, at the other extreme.[86] Plotted on the spectrum of possible liability schemes, the current system, the wide view of § 230 under *Zeran*, falls somewhere on the right (high immunity, low liability).

86. *See also* Lemley, *supra* note 59, at 15 ("There are four basic possibilities [for an online liability rule]: no safe harbor at all, complete immunity, a notice-and-takedown regime modeled on the DMCA, or a no-damages, no-interference regime modeled on the trademark statute.").



B. Reversion to Traditional Common Law Jurisprudence

One approach to liability for user-generated content assumes that the Internet is not fundamentally different than older media such that the best approach is simply to apply existing law—including defamation law and traditional First Amendment jurisprudence.[87] Advocates of the common law approach argue that § 230 cut short the natural adaptation of the law to the Internet, an adaptation that would incorporate trade-offs and value judgments that have refined over time.[88] Seemingly a member of this camp, Judge Easterbook famously compared the concept of cyberlaw generally to "the law of the horse"—implying both are ridiculous as independent bodies of law.[89] He argued that "[m]ost behavior in cyberspace is easy to classify under current [legal] principles," so, his argument goes, sound general legal principles provide the best framework for dealing with

87. *See, e.g.*, Jae Hong Lee, Note, Batzel v. Smith & Barrett v. Rosenthal*: Defamation Liability for Third-party Content on the Internet*, 19 BERKELEY TECH. L.J. 469, 485-87 (2004) (declaring that the internet is not too exceptional for traditional doctrines); GEOFFREY C. HAZARD, JR., ET AL., PLEADING AND PROCEDURE, STATE AND FEDERAL CASES AND MATERIALS 237-38 n.4 (9th ed. 2005) (explaining that, on the issue of personal jurisdiction, some "cases suggest . . . that a special intellectual framework for internet cases is unnecessary.").

88. *See, e.g.*, Lee, *supra* note 87, at 487-88 (arguing that Section 230 and *Zeran* "derailed the process" of common law evolving to address to the new technology of the Internet).

89. Frank Easterbrook, *Cyberspace and the Law of the Horse*, 1996 U. CHI. LEGAL F. 207, 207 (1996).

liability, contract, and property issues online.[90] In other words, according to him, cyberspace requires no specialized statutory framework.

Even if it might prove "easy,"[91] leaving the liability determination to the common law's jurisprudence of categories would have awkward, unacceptable repercussions. This is especially true given the complexities—post-dating Easterbrook's statement—that Web 2.0 adds regarding who creates content and what qualifies an actor as a publisher. A common law liability system would run counter to Congress's expressed intent. Furthermore, it would lead interactive service providers to create boundaries around their activities based on the activities' potential for legal categorization rather than their utility or other market-imposed measures. Finally, it would create legal uncertainty likely to chill speech.

1. The Stratton Oakmont Problem

Reverting to pre-Section 230 jurisprudence would force the absurd result in *Stratton Oakmont*, where a good faith effort to police message boards to protect children led to *more* liability for an internet service provider. Even the staunchest § 230 critics accept that in passing § 230, Congress sought to reverse this result and aimed to encourage interactive service providers to implement voluntary self-policing like that which *Stratton Oakmont* effectively penalized.[92]

Supporters of applying the common law tort liability approach argue that it would "encourage internet service providers to do their part" to prevent and lessen the impact of bad acts online.[93] Maybe so, but the problem

---

90. *Id.*

91. Though I accept Judge Easterbook's premise for purposes of this Note, the notion that adapting common law jurisprudence to the Internet proves "easy" is not necessarily true, or at least not self-evident. Challenges abound, including of jurisdiction, of scale, of privacy and anonymity and the lack of authentication (e.g., of a child's age), and of the problem of human versus automated action. *See generally* Lawrence Lessig, *The Law of the Horse: What Cyberlaw Might Teach*, 113 HARV. L. REV. 501 (1999) (responding to Easterbrook and pointing out the unique challenges to regulation that "cyberspace" presents versus "real" space presents).

92. *See* 141 Cong. Rec. H8468-72 (daily ed. Aug. 4, 1995).

93. Douglas Lichtman and Eric Posner argue that the CDA and robust immunity under it are "sharply inconsistent with conventional tort law principles" and therefore should be abandoned. They reason that ISPs are optimally positioned to reduce bad acts online and that imposing liability on them would match the offline jurisprudence, writing that "rules that hold one party liable for the wrongs committed by another are the standard legal response in situations where . . . liability will be predictably ineffective if directly applied to a class of bad actors, and yet there exists a class of related parties capable of either controlling those bad actors or mitigating the damage they cause." Douglas Gary Lichtman & Eric A. Posner, *Holding Internet Service Providers Accountable* 2-3 (U. Chi. L. & Econ. Olin Working Paper, No. 217, 2004), *available at*

with such an approach is that the abstract justification for strict liability applied to publishers of third-party content in traditional contexts would carry with it an unjustifiable burden on free speech in the online world. The efficiency rationale that justifies spreading the costs of injuries from a product or service to everyone who uses it, by holding its providers liable,[94] ignores the value of free speech and fails to appreciate the social utility of the Internet and its growth. Under strict liability, potential injurers (here, websites) completely internalize the marginal cost of precautionary measures, which gives them incentives to do so efficiently.[95] They reduce their risk to optimally reduce cost. That creates incentives that, as detailed below, have high costs for free speech and the value of the web, strengthening the argument for a robust immunity system on a societal level.

2. Category-based Liability Leads to Over-precaution by Risk Averse Providers

Online service providers might respond to the common law's category-based liability system by tailoring their services to avoid the semblance of editorial control, the consequence of which is more liability. For example, online providers might offer only the simplest tools and post content exactly as they receive it to avoid making editorial-type judgments about placement and display of it. This is true both of the distinction between publisher and distributor (i.e., the move from strict liability to liability on knowledge and negligence) and of the distinction between distributor and common carrier (moving from liability on knowledge/negligence to full immunity).

But the bigger problem is that, even if they wanted to, some online services simply could not make such adjustments. Search engines, for example, display results based on a scan of, and judgment concerning, the contents of the billions of web pages they index. The search-engine pro-

---

http://ssrn.com/abstract=573502 (joining "a growing chorus of legal commentators in arguing" for "legal rule[s] that bring[] Internet service providers (ISPs) into the chain of responsibility.") (citing sources).

94. *See, e.g.*, Escola v. Coca-Cola Bottling Co., 24 Cal.2d 453, 462 (1944) (Traynor, J., concurring) ("Even if there is no negligence, however, public policy demands that responsibility be fixed wherever it will most effectively reduce the hazards to life and health inherent in defective products that reach the market.").

95. ROBERT COOTER & THOMAS ULEN, LAW AND ECONOMICS 307-346 (4th ed. 2004), *available at* http://www.law.berkeley.edu/centers/bclbe/Courses/Law216/CooterUlen/216%20chpt8.pdf.

vider must make decisions about display based on content.[96] No matter how much a search engine provider relies on, or claims to rely on, automation rather than human editing, relevance, critical to a useful search engine,[97] is inherently subjective. To present "relevant" results, the search engine designers have to decide: relevant to whom, by what metric, and in what context?[98] One classic example cited in the search industry is the term "apple"—a good search engine should capably disambiguate whether the user seeks the computer company or the fruit.[99] For Google and others to be able to make that kind of distinction, and, based on it, reveal the web's content to millions of users requires a great deal of subjective judgment about not only the intent of the user but also about the meaning, message, and indeed the worth of the web's content (the pages in the search engine's index).[100] That kind of judgment is, under the common law jurisprudence, editorial control. Under the common law categories, then, editorial control means strict liability would thus apply to search engines. That fact alone troubles some scholars enough to call for special liability standards for search engines[101] or at least judicial and legislative caution with respect to them.[102]

Some argue that the *Stratton Oakmont* court got it wrong only in deciding that the *automated* filtering (e.g., for swear words) that Prodigy performed constituted editorial control.[103] But if courts were to address that

---

96. *See* Lemley, *supra* note 59, at 2 ("If we forced Google to try to find out which Web pages have problematic materials on them, there is no way it could return automated search results.").

97. Matt Hines, *The Future of Search Rides on Relevance*, CNET NEWS.COM, Jan. 29, 2005, http://www.news.com/2100-1032_3-5555954.html (explaining that industry executives "roundly endorsed the idea that making search tools more relevant in customers' lives will be the most important factor in driving their companies' success.").

98. Wilfred Ng, Lin Deng & Dik Lun Lee, *Mining User Preference Using Spy Voting for Search Engine Personalization*, 7 ACM TRANSACTIONS ON INTERNET TECHS. 1, 1 (Aug. 2007).

99. Steven Johnson, *Digging for Googleholes: Google May Be Our New God, But It's Not Omnipotent*, SLATE (Jul. 16, 2003) (highlighting search engines' "skewed synonyms" problem).

100. Even if Google and others try to minimize subjectivity by using tangible measures of relevance like the number of other websites linking to a particular site, the decision of which measures to weigh more heavily proves subjective, as do the search engine's necessary efforts at stopping fraudulent sites like link farms.

101. *See, e.g.*, Pasquale, *supra* note 58, at 136-42, 185-93 (advocating special treatment of search engines under the fair use doctrine).

102. *See* Grimmelmann, *supra* note 55, at 50 ("We need to analyze any serious proposal for a change in Internet law for its effects on the search ecosystem.").

103. *See, e.g.*, Butler, *supra* note 34, at 256-57 ("The source of the confusion over the liability of ISPs as publishers is the *Stratton Oakmont* decision that clumsily applied a

concern by, for example, requiring manual human editing before a provider transitioned to publisher from distributor status, that too would prove problematic. It would strongly favor providers that deployed fully-automated systems (and had the technical/financial resources to do so), rather than those that might use human editors to try an improve quality. Such a system would also lead to difficult issues around when human editing actually occurs, e.g., if a spam filter "learns" from human input, has the content that the filter assesses been human-edited? Astute commentators have also pointed out that human programmers write the algorithms that do the editing anyway, so such a distinction seems contrived anyway.[104]

Even if courts sometimes classified service providers as mere distributors requiring a showing of knowledge or negligence before liability attached,[105] the uncertainty of qualifying for the preferable distributor status would still result in service provider over-precaution and its accompanying chilling effect on free speech.[106] In the abstract, uncertainty in a liability system allows actors to reduce the chance of punishment by "playing it safe," so it leads actors to modifying their behavior more than the law requires.[107] As a result, even risk-neutral parties tend to "over-comply."[108] Again, that will make providers less likely to manipulate content in interesting, innovative, and beneficial ways. If a given design tweak, for example, would make a service only somewhat more interesting and engaging but would require some kind of editorial input, a provider likely will not

---

fault standard best suited for newspapers and book publishers upon Prodigy, merely because Prodigy attempted to provide a small measure of order and control over the content of its electronic bulletin boards.").

104. James Grimmelmann, *The Structure of Search Engine Law*, 93 IOWA L. REV. 1, 60 (2007).

105. This was the result in a pre-Section 230 case, *Cubby Inc. v. CompuServe Inc.*, 776 F. Supp. 135 (S.D.N.Y. 1991).

106. Before § 230, providers in fact worried of uncertainty under existing liability rules. *See* Luffman, *supra* note 79, at 1071-73 (collecting "apocalyptic reactions" to *Stratton Oakmont*); *see also* Steve Alexander, *The Content of Cyberspace; By editing, MRNet may have weakened its disclaimer that it is not responsible for Internet content that moves on its wires*, MINN. STAR TRIBUNE, Jan. 5, 1996, at 3B (quoting director of ISP trade association saying, "[t]he legal situation is foggy and gray and it's likely to be for the next couple of years.").

107. Richard Craswell & John E. Calfee, *Deterrence & Uncertain Legal Standards*, 2 J. LAW, ECON. & ORG. 279, 279-83 (1986)

108. *Id.* at 280.

implement it.[109] The marginal effect—that some providers will avoid creating new Web 2.0 services to avoid liability—potentially cuts off the "long tail" and eliminates much of the social value of the Web 2.0. One scholar sums it up nicely: "under such a regime, the Internet might be about where digital cable systems are, with lots of downstream content and very little opportunity for interactivity, much less individual publishing."[110]

C. Attaching Liability Upon Knowledge or Notice

This Section argues that even if online service providers' status as distributors were certain, if liability attached to providers upon knowledge or notice, problems would abound. Section III.C.1 considers the negative effects of a scheme attaching liability upon knowledge, while Section III.C.2 identifies problems with attaching liability upon actual notice.

1. Using Common Law/Pre-CDA Definitions of Knowledge

Courts could implement a knowledge-triggered liability system without congressional action by reverting to the common law distributor liability standard (i.e., by discarding the *Zeran* court's controversial reading of § 230's "treatment as a publisher" as precluding distributor liability).[111] Attaching liability upon knowledge or notice would create serious problems for Web 2.0 companies, however, because under the standards developed in pre-internet defamation cases, they would likely qualify as having "knowledge." Under those standards, knowledge is defined as knowing or having reason to know of content's illegal character.[112] Offline distributors like, for example, Borders Bookstore, simply do not have that problem; offline distributors do not and could not realistically scan the content of, for example, every magazine they sell. Courts have recognized

109. Notably, though, even relatively certain qualification for distributor liability status would pervert the web's growth; I discuss the problems with knowledge or notice-based systems in more detail below. *See infra* Section III.C.2.

110. Jim Harper, *Against ISP Liability*, 28 REGULATION 30, 33 (Spring 2005), *available at* http://ssrn.com/abstract=807545.

111. *See Zeran*, 129 F.3d at 330 ("By its plain language, § 230 creates a federal immunity to any cause of action that would make service providers liable for information originating with a third-party user of the service."); Chang, *infra* note 45, at 983-87 (explaining the alternative reading of § 230 under which distributor liability persists).

112. *See* Lerman v. Chuckleberry Publ'g, Inc., 521 F. Supp. 228, 235 (S.D.N.Y. 1981) ("[C]ourts have long held that vendors and distributors of defamatory publications are not liable if they neither know nor have reason to know of the defamation.").

as much.[113] In fact, courts offer that as a key reason for the appropriateness of imposing liability on knowledge.[114] Courts reason that imposing liability on any lesser showing than knowledge would lead to self-censorship.[115]

However, the same standard works differently online than offline. Under such a standard, a search engine's mere scanning of web pages, even without any decision (whether by editor or algorithm) as to whether to display the pages in search results, leads the search engine to "know or have reason to know" the web page's content and character. Going forward, advanced technology like semantic analysis, concept-mapping, and natural language search will increasingly make it impossible for sites to claim lack of knowledge of the content to which they provide access.[116] A concrete example illustrates the point. Google's director of research talks about a day when the search engine will be able to handle the query: "show me the speech where so-and-so talks about this aspect of Middle East history."[117] For Google to return a meaningful response to the query would be tremendously valuable to users. But to do so, Google would certainly have to know or have reason to know what the content means or implies.

Sites would thus seek to avoid "knowledge" of risky content. The search engine space proves particularly vulnerable under such a standard. Search engines might abandon indexing any unknown content. They might require people to submit their sites and agree to indemnify the search engine and only index those sites whose operators agree, effectively eviscerating internet-wide search, slowing the growth of the Web, and silencing many of the web's users in the process. Or, they might restrict searches for illegal or defamatory content, as they must do in China today.

---

113. Smith v. Cal., 361 U.S. 147, 153 (1959) ("[I]f the bookseller is criminally liable without knowledge of the contents, and the ordinance fulfills its purpose, he will tend to restrict the books he sells to those he has inspected.").

114. *Id.*

115. *Id.* ("[D]ispensing with any requirement of knowledge of the contents of the book on the part of the seller . . . tends to impose a severe limitation on the public's access to constitutionally protected matter.")

116. For a comprehensive review of the state and future of search technology and related academic research, see conference materials and archived video presentations from The Future of Search, University of California, Berkeley CITRIS-NERSC Sponsored Research Event, http://www-bisc.cs.berkeley.edu/FutureSearch/ (last visited Jan. 20, 2008).

117. Kate Greene, *The Future of Search: The head of Google Research talks about his group's projects*, MIT TECH. REV., Jul. 16, 2007, http://www.technologyreview.com/Biztech/19050/.

Beyond search, activities like setting up topical message boards or featuring content based on algorithmic calculations of popularity and other metrics would also be hindered because they require the entity providing them to know something about the content itself. Flickr's popular "Most Interesting" photos feature,[118] for example, relies on a constantly-updated variety of ever-changing metrics, including the source of clicks and comments to a photo and whether and how users tag or mark it as a favorite.[119] An enterprising plaintiffs' lawyer could, for example, find a link between these metrics and the illegality of the "interesting" photos the algorithm returned—e.g., that interesting photos are more likely to be tortious, and that Flickr designed its algorithm as such and thus encouraged users to engage in tortious behavior. In such a case, it would be difficult for Flickr to say it does not "know" that it encourages, or at least more actively promotes, tortious over non-tortious content.

2. Using a Formal Notice-based Liability Scheme like the DMCA

A formalized system akin to the notice-and-takedown safe harbor in the Digital Millennium Copyright Act[120] would address the problem of what constitutes "knowledge." It would also avoid the "electronic scanning equals knowledge" problem outlined above. Such an approach finds many proponents in academia[121] and in at least one (since overruled) court.[122] A formal notice-based system, proponents argue, would give injured parties a mechanism to request removal of offending content and service providers an incentive to take that content down—an incentive they argue that § 230 fails to provide. Nonetheless, even a formal notice-based system would have negative effects that outweigh its (debatable) potential benefits.[123]

---

118. Explore, http://www.flickr.com/explore/ (last visited Oct. 28, 2007).

119. About Interestingness, http://www.flickr.com/explore/interesting (last visited Jan. 20, 2007).

120. *See* 17 U.S.C § 512 (2000).

121. *See, e.g.*, Lee, *supra* note 87, at 491-92 (arguing for a "regime . . . analogous to the notice-based system established under the Digital Millennium Copyright Act."); Ryan W. King, *Online Defamation: Bringing the Communications Decency Act of 1996 in Line with Sound Public Policy*, 2003 DUKE L. & TECH. REV. 24 (2003); Butler, *supra* note 34, at 262-63 (proposing a notice-and-takedown process for defamation "similar to the one used for potential copyright violations in the Digital Millennium Copyright Act" and arguing that "[s]uch a procedure could work effectively" and "the process would be simple.").

122. *See* Barrett v. Rosenthal, 114 Cal. App. 4th 1379, 1403-06 (2004).

123. The premise that businesses have no incentive to police content under Section 230 seems flawed. Websites have a business incentive, if not a legal one, to keep subscribers happy and the content on their sites legal. Indeed Congress explicitly wanted to

a) The Marginal Cost of Postings Problem

First, such a system would have precisely the consequences the *Zeran* court predicted in justifying its broad interpretation of § 230.[124] If providers are "[f]aced with potential liability for each message republished by their services," they will respond by restricting the amount of type content they are willing to republish.[125] Economics again requires this result.[126] When each additional message posted on a site brings no or very little additional liability (the result under § 230 today), then the marginal cost to a site of each new posting continues to fall and indeed approaches zero, or at least a predictable step-curve wherein a certain number of new messages requires the provider to obtain new servers. Each new user-created post, message, or tag, costs less than previous ones, so providers can allocate the fixed development costs of the entire system across each new posting. That truly enables Web 2.0's "long tail"—the billions of pages on the web, the fact that search engines can handle billions of queries to return those billions of pages in results, and that operators like Craigslist can maintain message boards with over 75 million postings in over 100 categories.

In contrast, under a notice-based system, the marginal cost of each posting never goes to zero because each post represents some fixed percentage chance of legal liability, plus some cost of compliance (of responding to takedown notices). Especially for a site like Craigslist, which does not charge or collect revenue per post, the effect could be major: the site might simply stop accepting posts at the point that it cannot reasonably respond to the volume of notices in a way that complies with the DMCA-like notice-system. By keeping the marginal cost of each new post high, then, a notice-based system would destroy the promise of Web 2.0 (that the value of the network depends on its volume of users and their engagement). In other words, under a liability-on-notice system, providers will be less likely to expand the network, thus reducing its value to all participants.[127]

---

encourage this sort of self-policing by passing Section 230. *See* 141 Cong. Rec. H8469 (daily ed. Aug. 4, 1995).

124. *See Zeran*, 129 F.3d at 331.

125. *Cf. id.*

126. *See* Seth F. Kreimer, *Censorship by Proxy: The First Amendment, Internet Intermediaries, and the Problem of the Weakest Link*, 155 U. PA. L. REV. 11, 29-30 (2006) (explaining that economics makes "intermediaries . . . particularly susceptible to chill" with respect to speech, and that they are often willing to cause some "collateral damage to protected expression" in exchange for avoiding liability).

127. *See* Metcalfe, *supra* note 76 (explaining that the value of a network, social and otherwise, grows as roughly the square of its number of users).

b) The Incentive to Chill Speech and the Related Constitutional Problem

In addition to the marginal cost problem, differences between the types of offenses the DMCA system targets and the third-party behavior for which § 230 provides immunity today render a notice-based system constitutionally and practically unworkable beyond the copyright realm.[128] A takedown notice under the DMCA is a clear and easy-to-prepare document,[129] and response to it requires relatively little judgment by its recipient, or at least, that is the premise DMCA supporters cite.[130] In contrast, notices in the CDA/Section 230 context could allege any of hundreds of torts under hundreds of state and federal laws with slight variations among them, so the notices would be harder to prepare and interpret.[131] Even scholars who support such a system admit that this key practical difference makes such a system less appropriate beyond the copyright realm.[132] Furthermore, even within the relatively clearer copyright context, empirical evidence indicates that more than a quarter of DMCA takedown notices are either on shaky legal grounds or address cases in which no copyrights are violated.[133] Anecdotal evidence concurs, with at least one major online provider publicly declaring that "[w]hat we have to do is take [DMCA notices] at face value . . . our responsibility is to abide by the notices . . . ."[134] Outside the copyright context, taking a legal claim at face value means

128. This argument holds regardless of one's feelings about how well the DMCA notice-and-takedown system works in addressing the problem of online copyright infringement.

129. *See* 17 U.S.C. § 512(c)(3) (2000).

130. *See* Jennifer Urban & Laura Quilter, *Efficient Process or 'Chilling Effects'? Takedown Notices Under Section 512 of the Digital Millennium Copyright Act*, 22 SANTA CLARA COMP. & HIGH TECH L.J. 621, 640-41 (2006) ("If notices are generally sent when copyright infringement is clear-cut—the assumption behind the positive story of the DMCA—Section 512 may represent an efficient way to clear infringing materials from the Internet.").

131. *See* Bradley A. Areheart, *Regulating Cyberbullies Through Notice-Based Liability*, 117 YALE L.J. POCKET PART 42 (2007), http://thepocketpart.org/2007/09/08/areheart.html (noting the variety of claims related to third-party content for which the CDA gives service providers immunity).

132. *See id.* (after advocating for a notice-and-take down system, explaining that it should "only allow redress for torts that have relatively unambiguous elements" and calling for "principled demarcation" of a few specified torts.); Butler, *supra* note 34, at 264 (2000) (admitting that "[i]t is much easier for ISPs to judge whether a copyrighted work has been violated . . . than whether a factual assertion is defamatory.").

133. Urban & Quilter, *supra* note 130, at 667-78.

134. Jim Avila, et al., *The Home Video Prince Doesn't Want You to See*, ABC NEWS INTERNET VENTURES, Oct. 26, 2007, http://abcnews.go.com/print?id=3777651 (quoting Ricardo Reyes, a spokesman for Google-owned online video service YouTube).

taking down essentially any content in response to any complaint. Rather than expend resources investigating these claims, then, interactive service providers will likely just take down the content.[135] One could even envision an automated system allowing users to remove content themselves, e.g., via a hyperlink asking, "do you have a legal claim related to this post? Click here to remove it."

Such a system would fly directly in the face of Supreme Court precedent on free speech. It would create an extreme version of the impermissible "heckler's veto"[136]—giving anyone with the desire the ability to silence another's speech and engage in mass censorship.[137] Arguably, incorporating features like those of the DMCA notice-and-takedown system, requiring complainants to certify their legal claims on penalty of perjury[138] or setting up a formal counter-notice system,[139] could help avoid such a result.[140] Still, serious questions about the efficacy of the countermeasures in the DMCA system linger,[141] and moreover, most of the damage to free speech occurs upon takedown because of the instantaneous nature of communication online. Also in the copyright setting, the Supreme Court has warned that, where decisions to remove or forbid challenged content implicate free speech, they require very careful "case by case analysis"[142] and a "sensitive balancing of interests."[143] Considering that courts struggle with them, leaving these delicate issues of constitutional judgment to non-lawyer ISP employees motivated by the company's bottom line rather than substantive justice or even to just users themselves would have impermis-

135. Barrett v. Rosenthal, 40 Cal. 4th 33, 54-55 (2006) (citing "three deleterious effects that would flow from reading section 230 to permit liability upon notice," including its creation of an incentive for ISPs to immediately takedown challenged content.)

136. *See* Reno v. ACLU, 521 U.S. 844, 880 (1997).

137. *See* Donato v. Moldow, 865 A.2d 711, 726 (N.J. Super. Ct. App. Div. 2005) ("If notice could defeat immunity, anyone in any way 'displeased' with posted materials could utilize notice as a 'no-cost' means to create the basis for future lawsuits."). *But see* Areheart, *supra* note 131, at 45 (arguing that a notice-based system would "achieve[] the '[p]recision of regulation' that the Supreme Court has required for rules implicating the First Amendment.") (quoting NAACP v. Button, 371 U.S. 415, 438 (1963)).

138. 17 U.S.C.S. § 512(c)(3) (2008).

139. 17 U.S.C.S. § 512(g)(1) (2008).

140. *See* Butler, *supra* note 34, at 262-63.

141. *See* Urban & Quilter, *supra* note 130, at 666 (presenting results from an empirical study of § 512 takedown notices and concluding that at least one-third of notices were flawed and therefore "invite[d] serious concerns about the fairness of the process . . .").

142. Campbell v. Acuff-Rose Music, 510 U.S. 569, 581 (1994).

143. *Id.* at 584; Sony Corp. v. Universal City Studios, Inc., 464 U.S. 417, 455 n.40 (1984).

sible chilling effects.[144] Even if an ISP employed "an army of lawyers," it would not be able to adequately tell what content should legally stay up and which it should remove.[145] As a result, to avoid liability, companies would err on silencing speech. Finally, as explained above, such a generalized online liability system would be practically harder to administer than the DMCA has been for copyright amplifies the Constitutional problem.

c) Defamation and Other Forms of Liability Differ from Copyright, So the DMCA Model Does Not Easily Extend

Beyond the practical differences, defamation and other torts from which § 230 protects online providers do not share the free speech "saving grace" that copyright law has been held to enjoy. Copyright law itself encourages, and was constitutionally created to encourage, free expression.[146] In contrast, as the Supreme Court has said, libel law has no such beneficial intent or effect on free speech—its role "has been relatively minor and essentially erratic."[147] Other kinds of third-party content claims the CDA has been held to bar against online service providers, like securities law claims[148] or business practices regulations,[149] likely warrant even less constitutional indulgence than libel law. A DMCA-like liability system to replace § 230, then, would be unlikely to withstand Constitutional scrutiny because of its implications for free speech.[150] That problem, com-

144. The Supreme Court has affirmed the delicacy of these kind of judgments even at the procedural level. *See* Bose Corp. v. Consumers Union, 466 U.S. 485, 499 (1984) ("[I]n cases raising First Amendment issues we have repeatedly held that an appellate court has an obligation to make an independent examination of the whole record in order to make sure that the judgment does not constitute a forbidden intrusion on the field of free expression.") (internal quotations and citations omitted). That the Supreme Court finds even federal district courts incapable of making these decisions cautiously enough is telling.

145. *See* Lemley, *supra* note 59, at 2.

146. *See, e.g.*, Harper & Row, Publ'rs. v. Nation Enters., 471 U.S. 539, 558 (1985) ("[T]he framers intended copyright itself to be the engine of free expression."). *See also* Eugene Volokh, *Freedom of Speech and Appellate and Summary Judgment Review in Copyright Cases*, 107 YALE L.J. 2431, 2488 (1998) ("Copyright law's speech-enhancing effect, coupled with its specific constitutional authorization, justifies holding copyright law to be a substantively valid speech restriction.").

147. *See* Gertz v. Robert Welch, 418 U.S. 323, 400 n.41 (1974) (citing T. Emerson, THE SYSTEM OF FREEDOM OF EXPRESSION 519 (1970)).

148. *See* Universal Commc'n Sys. v. Lycos, Inc., 478 F.3d 413 (1st Cir. 2007).

149. *See* Stoner v. eBay, 56 U.S.P.Q. 2d. 1852 (Cal. Super. Ct. 2000).

150. In considering a challenge to a new liability system affecting free speech, the Supreme Court would apply First Amendment tests for overbreadth and vagueness, under which regulations fail where their "burden on protected speech . . . could be avoided by a more carefully drafted statute." *Cf.* Reno v. ACLU, 521 U.S. 844, 848 n.45, 868, 871-874

bined with the likely detrimental effects on Web 2.0 and the Internet generally, makes the regime of § 230 under *Zeran* preferable.

D. *Grokster*'s "Affirmative Steps" Standard and Other Intent-based Tests

Moving to the right on the liability-immunity spectrum from notice-based liability leads to systems that impose liability on online service providers for the content of others only when the providers have some higher level of scienter related to the content or its illegality. One judge suggested adopting criminal law's traditional test for liability, i.e., finding an actor responsible who has some intent to aid and abet the target behavior.[151] A creative plaintiff[152] called for extending the Supreme Court's *Grokster* standard for copyright infringement inducement, under which on who makes "clear expression or [takes] other affirmative steps . . . to foster infringement, is liable for the resulting acts of infringement by third parties,"[153] to all liability arising from third-party generated content online. Such tests have some appeal: They would impose liability on the worst online service providers—sites that, intuitively anyway, seem to deserve to face liability. The Ninth Circuit recently put forth such an example—the hypothetical "www.harassthem.com."[154] Under a broad reading of § 230, such a site might retain immunity from claims of injury resulting from harassing messages users posted on the site, even if the site encouraged users to create such illegal content.

Still, the potential for a *Grokster*-based system to chill speech still exists, and the same issues that make the DMCA-takedown model inappropriate beyond copyright apply with nearly equal force. Providers who set up online communities want the value of those communities to increase, they make more money when traffic increases, and the value of the network increases not only for users but also for providers as postings increase. The same could have been said for music exchange service Grokster and copyright infringement, but again, the key practical and Constitutional differences outlined above between online liability generally and copyright liability make the *Grokster* test a bad fit. If the dispositive question becomes not whether a provider created a piece of content but whether it intended for content to go up, the answer would almost invaria-

---

(1997) (applying the doctrines in the context of a content-based regulation, subject to strict scrutiny).

151. *Stoner*, 56 U.S.P.Q. 2d. 1852, *14-*15 (Cal. Super. Ct. 2000).

152. *See Universal*, 478 F.3d at 420-21.

153. *See* Metro-Goldwyn-Mayer Studios, Inc. v. Grokster, 545 U.S. 913, 919 (2005).

154. Fair Hous. Council of San Fernando Valley v. Roommates.com, LLC, 489 F.3d 921, 928 (9th Cir. 2007), *rev'd en banc*, 521 F.3d 1157 (9th Cir. 2008).

bly be yes—effectively eviscerating immunity overall, making liability strict, and leading to the necessarily accompanying chill on free speech.

E. Other Possible Systems

In the last several decades, scholars have had ample opportunity to consider how liability schemes should attach to new technologies and have proposed a variety of ideas. Some proposals involve systems that would force interactive service providers to disclose the identities of the creators of offending content.[155] That way, the logic goes, the law would enable potential plaintiffs to find and hold responsible those who actually cause the problem. However, requiring online providers to maintain records of every posting online would be a massive undertaking unreasonable to impose. Further, such a system would effectively prevent anonymous posting,[156] a constitutional right that courts have recognized as critical to free speech online and otherwise.[157] Professor Mark Lemley suggests a system based on the trademark statute,[158] but the complete lack of case law interpreting the applicable portion of the statute[159] makes such a system difficult to evaluate.

Another commentator sets forth a creative proposal for dealing with the problem of third-party content liability online—essentially an online 'right of reply' system for search engines.[160] The proposal would require Google and others to allow users to "asterisk" search results displaying content they felt harmed them and the ability to post a reply to it.[161] The proposal has the advantages of providing injured parties with some redress when they seek to challenge third-party content and of addressing some people's intuitive sense that "*some* accountability for search engine results

---

155. *See, e.g.*, Ehrlich, *supra* note 8, at 402 (proposing "[c]ombining immunity with a remedy that allows plaintiffs to reach the actual publisher . . . ."); Lemley, *supra* note 59, at 21-22 (outlining a system "requiring intermediaries to retain and disclose the identity of their customers in response to a subpoena.").

156. *See* Lemley, *supra* note 59, at 15.

157. *See, e.g.*, Doe v. 2themart.com, Inc., 140 F. Supp. 2d 1088, 1092 (D. Wash. 2001) ("A component of the First Amendment is the right to speak with anonymity. This component of free speech is well established. . . . The right to speak anonymously extends to speech via the Internet."); ACLU v. Miller, 977 F. Supp. 1228, 1230-32 (N.D. Ga. 1997) (recognizing right to speak anonymously on the Internet); *see generally* McIntyre v. Ohio Elections Comm'n, 514 U.S. 334 (1995) (decision to remain anonymous is protected by the First Amendment).

158. *See* Lemley, *supra* note 59, at 19.

159. 15 U.S.C. § 1114(2)(B)-(C) (2000).

160. Frank Pasquale, *Rankings, Reductionism, and Responsibility*, 54 CLEV. ST. L. REV 115, 135-36 (2006).

161. *Id.*

is increasingly necessary as they become the primary portal for net users."[162] To the extent that it is, as its proponent claims, "a minor, non-intrusive legal remedy," it might not prove problematic provided that the § 230 immunity otherwise continues to apply as it does today. Still, the measure seems like a stop-gap, and it might not be practicable as applied to alternative forms search (e.g., voice search, map search, mobile search). Besides, there is no guarantee that searchers will actually click on the asterisks, so the defamed person likely will not feel this approach makes him whole.

F. *Zeran* and a Broad Interpretation of § 230 Have Allowed Web 2.0 Models to Flourish

The *Zeran* regime has not had negative consequences for free speech and innovation online likely under the systems discussed above. As this Section argues, *Zeran* has proven efficient[163] and adaptable and nurtured the growth of beneficial innovation online. It has effectuated Congressional intent to "promote the continued development of the Internet and other interactive computer services."[164]

1. Search Engines

The search space demonstrates the point well. As explained above, internet search is inherently editorial—even if algorithms do the editing—because it involves content-based decision-making as to relevance, display and usability. Systems that, unlike § 230 under *Zeran*, bias against editorial functions in determining liability thus risk hindering search. Section 230, on the other hand, explicitly precludes liability for "acting as a publisher," i.e., exercising editorial control over content posted online, so search engines are free to do what they need to do to operate.

Search engine cases that follow *Zeran* bear out that conclusion. In *Murawski v. Pataki*, the court held that search engine Ask.com was immune under § 230 from defamation claims relating to content presented in search engine results.[165] Citing *Zeran*, the court found immunity, notwithstanding that the search engine removed line breaks in the results in such a way that it appeared plaintiff was associated with the Communist Party,

---

162. *Id.* (emphasis in original).

163. For an extended analysis of just the economic aspects of the available liability systems, see Matthew Schruers, *The History and Economics of ISP Liability for Third Party Content*, 88 VA. L. REV. 205, 206-08 (2002) ("[R]elative to the available alternatives, the current regime, in which ISPs are almost completely immune from suit, is the most efficient.").

164. *See* 47 U.S.C. § 230(b)(1) (2000).

165. 514 F. Supp. 2d 577, 591 (S.D.N.Y. 2007).

even though it did not so appear on the destination sites from that created the content.[166] Likewise, the court in *Langdon v. Google, Inc.* held that § 230 immunized Google and Yahoo! from claims arising from any "decisions relating to the monitoring, screening, and deletion of content from their network[s]," including whether and how they displayed ads and results based on their content.[167] The court explained that under *Zeran* and its progeny, § 230 "bars lawsuits seeking to hold a service provider liable for . . . deciding whether to publish, withdraw, postpone, or alter content."[168]

2. Non-search Providers

Under *Zeran*, non-search providers also enjoy wide latitude in how they design their sites and display and manipulate user-generated content. The court in *Donato v. Moldow*, for example, discussed *Zeran*'s interpretation of § 230 at length and held that, under it, a local-issues website operator was immune from plaintiff's claims of injury from messages posted on its site.[169] The court reached that conclusion, despite plaintiff's contention that defendant controlled and shaped the tone and content of the message board by choosing to display, highlight, and comment on certain messages but not others.[170] According to the court, "selectively choosing which messages to delete and which to leave posted" on a message board was mere "exercise of a publisher's traditional editorial functions, namely, whether to publish, withdraw, postpone or alter content provided by others."[171]

In *Universal Communication Systems v. Lycos, Inc.*, the court cited *Zeran* for the proposition that mere notice does not change the analysis because § 230 precludes distributor liability.[172] The court dismissed plaintiff's claims otherwise.[173] What makes the case interesting is that instead of alleging that defendant Lycos was directly responsible for the content of message board postings—a claim that § 230 obviously proscribed—the plaintiffs alleged that Lycos's *design* of its website harmed the plaintiff by enabling posters to the site to spread false information more credibly.[174]

---

166. *Id.* at 589-91.
167. 474 F. Supp. 2d 622, 630-31 (D. Del. 2007).
168. *Id.* at 630.
169. 865 A.2d 711, 725-26 (N.J. Super. Ct. App. Div. 2005).
170. *Id.*
171. *Id.*
172. 478 F.3d 413, 420-21 (1st Cir. 2007).
173. *Id.*
174. *Id. Cf.* Carafano v. Metrosplash.com, Inc., 339 F.3d 1119, 1121, 1124-25 (9th Cir. 2003) (holding website operator immune under § 230 when an anonymous poster

Specifically, the plaintiffs pointed to various things Lycos did to give the site, and the investment advice that users posted to it, an improved air of authority so as to "culpably assist" the creators of the offending content. The First Circuit called the strategy 'artful pleading' that failed to avoid the fact that the plaintiffs attempted to hold Lycos liable for content created by another.[175] Though the court ruled on the facts (that there was no active inducement by Lycos and therefore no reason to even consider not applying § 230 immunity), it opined in dicta that "[i]t is not at all clear that there is a culpable assistance exception to Section 230 immunity."[176] *Zeran* was not binding, for *Universal* was the First Circuit's first § 230 case.[177] Nevertheless, the court reviewed and agreed with *Zeran*'s more controversial holdings, and, importantly, did so in a way that protects online provider's ability to tailor their sites in ways that might affect the content, or the impact of the content, that users provide. That protection of that discretion provides online providers the ability to create new and innovative online experiences, without worrying about losing § 230 immunity for the user-generated content that underlies them.

3. Content Distribution

Reading § 230 to preclude distributor liability also critically supports Web 2.0's open content distribution model. Without that interpretation, a case like *Prickett v. infoUSA, Inc.*[178] would likely have come out differently. Defendant *info*USA operated an online directory listing service akin to the yellow pages.[179] A third party submitted a false listing to *info*USA for an escort service at the plaintiff's address, and the plaintiff alleged that he and his family suffered harassment as a result.[180] The court held *info*USA did not become an information service provider thereby and lose § 230 immunity for the content of the listing despite its licensing, categorization, tagging, and distribution of it to third parties.[181] That holding protects the mashup and data distribution services many laud as critical to the

created a false profile of the plaintiff on the defendant's dating website despite fact that the prankster merely filled in defendant's online forms to do so).

175. *Universal*, 478 F.3d at 420-21.

176. *Id.* at 421.

177. *Id.* at 418.

178. No. 4:05-CV-10, 2006 U.S. Dist. LEXIS 21867 (E.D. Tex. Mar. 30, 2006).

179. *Id.* at *7-8.

180. *Id.* at *8-10.

181. *Id. Cf. Carafano*, 339 F.3d at 1121, 1124-25 (9th Cir. 2003) (holding the provider of an online dating service immune under § 230 from harassment claims arising from third party's submission of a bogus profile including plaintiff's contact information, even though the site prompted and provided forms for the third party to create and submit the profile).

future of the Web.[182] If courts went the other way and discarded *Zeran*'s critical (and criticized) holding that § 230 precludes distributor liability, it would mean that by creating APIs and redistributing the user-generated content they control, services like *info*USA, Google AdSense, YouTube, and Flickr would lose § 230 immunity. Such a result would be disastrous for Web 2.0. It would force a reversion to the "walled garden"-style internet services of the late 1990's in which portal sites like AOL strived to keep users within their world and keep others' content out.[183]

4. Advertising

The *Zeran* framework also allows another behavior critical to the growth of online services that alternative systems likely hinder—websites' ability to make money generally and specifically from content-related advertising. For example, the court in *Doe v. Bates* held that defendant Yahoo! Inc. did not lose § 230 immunity despite generating significant advertising revenue from display ads placed near its popular Groups feature, even where users posted obviously illegal content to the groups.[184] In Web 2.0, internet services will increasingly provide targeted advertising based on the user-generated content of particular pages.[185] In fact, analysts consider offering services to users for "free" but making money by enabling advertisers to reach those users based on the content of the pages they view and the searches they perform as the web's most successful business model.[186] Thus, a system that threatened it would almost certainly harm the web's growth. Though no doubt self-serving, Google has cogently ar-

182. *See* Lin, *supra* note 72, at 101-102 (discussing the importance of mashups, search engines, and recommender systems).

183. *See generally* Michael Geist, *Pull Down the Walled Gardens*, BBC NEWS, Aug. 15, 2007, http://news.bbc.co.uk/go/pr/fr/-/1/hi/technology/6944653.stm (lamenting that today's social networks are somewhat of a reversion to the "walled gardens" of the late 90's but that today's sites' are willing to open up via platforms and APIs, a development he sees as a good thing).

184. Doe v. Bates, No. 5:05-CV-91-CF-CMC, 2006 U.S. Dist. LEXIS 93348, *9-12 (E.D. Tex. Dec. 27, 2006).

185. *See* Zachary Rogers, *Google Targets Search Ads on Prior Queries, à la Behavioral*, CLICKZ, Jul. 31, 2007, http://clickz.com/showPage.html?page=3626593. Arguably, such services improve the user experience because the ads shown are more relevant to them.

186. *See id.*; *see also* Dave Pollard, Why Google's Business Model Is So Revolutionary, SALON, Oct. 16, 2005 (How To Save The World Blog), http://blogs.salon.com/0002007/2005/10/16.html.

gued that its distributed advertising system itself promotes free speech by giving bloggers the ability to monetize their sites.[187]

In sum, the relatively low level of liability for third-party content possible under *Zeran* does not seem to at all hinder internet growth (and in fact enables it) in at least four areas critical to Web 2.0: search, content display and manipulation, content distribution, and the ability to rely on advertising revenue. As outlined above, the same certainly does not hold true of other potentially liability frameworks. That would seem to heavily favor leaving courts to continue to interpret § 230 expansively, especially in light of the web's aforementioned value in fostering free speech and social value of Web 2.0.

G. The Potential Problems With the *Zeran* Regime Are Not Unique to the Internet

Despite these benefits, the *Zeran* framework does have costs. It can sometimes result in unfortunate victims, who, especially when the original provider of the information at issue evades identification, pay the price for the free speech and growth that the *Zeran* regime enables. The plaintiff in *Zeran* himself so suffered; he was harassed as a result of the false information about him posted on AOL, and he received no compensation because AOL was immune he was unable to identify the original content provider.[188] Such unfortunate victims of free speech exist offline too, where the First Amendment likewise requires limits on impositions of liability that would dampen free speech.[189] Evaluations of the rationales for free speech as a fundamental right exceed the scope of this Note, but suffice it

187. Alan Davidson, Google Senior Policy Counsel, Google Inc. Letter re: FTC Town Hall, http://blog.wired.com/27bstroke6/files/google_town_hall_lecture.pdf ("[O]nline advertising promotes freer, more robust, and more diverse speech . . . website owners can afford to dedicate themselves to their sites more fully . . . because a significant percentage of the revenue we earn ends up in their hands as publishers of blogs and other websites and our advertising partners.").

188. *Zeran*, 129 F.3d at 329-330 & n.1.

189. *See* Frederick Schauer, *Uncoupling Free Speech*, 92 COLUM. L. REV. 1321 (1992) (arguing that First Amendment law need not presuppose a trade-off between tolerating individual harm and protecting societal free speech). "It ought to be troubling," Schauer argues, "whenever the cost of a general societal benefit must be born exclusively or disproportionately by a small subset of the beneficiaries . . . . If free speech benefits us all, then ideally we all ought to pay for it.". *Id.* at 1322. Schauer cites two forceful illustrations of "unfortunate victims" of offline free speech: *Herceg v. Hustler Magazine, Inc.*, 814 F.2d 1017 (5th Cir.1987) (holding publishing article was not incitement where teen died practicing auto-erotic asphyxiation technique described in magazine), and *Olivia LV. v. Nat'l Broadcasting Co.*, 178 Cal. Rptr. 888 (Ct. App. 1981) (holding television show producers not liable for incitement with respect to rape that perpetrators carried out based on TV show). *See id.* at 1323-24, 1343-49 (discussing cases).

to say that the Supreme Court has explained that free speech is paramount to American democracy.[190] Indeed, First Amendment defamation jurisprudence, which requires a showing of actual malice before any recovery for defamation of public figures,[191] and a heightened requirement of "clear and present danger" before even speech inciting illegality can be curtailed, shows that the law has considered and chosen to make difficult tradeoffs to protect free speech. That notion should extend to the web, especially in light of its Supreme Court-recognized power to promote free expression.[192]

Some commentators take issue with the free-rider problem that the *Zeran* system and Web 2.0 potentially entail: Companies like Google make money from other people's content but do not have to pay for it in the form of liability or otherwise.[193] That problem, again, is not unique to the Web. Booksellers and phone companies, both of which enjoy relaxed liability standards for third party content, make money from third party content too.[194] The fact that that internet companies at this point still do not capture the full social value of their sites[195] and the that the web is still in its relative infancy effectively counter this potential free-rider problem.[196]

---

190. *See generally* ERWIN CHEMERINSKY, CONSTITUTIONAL LAW: PRINCIPLES AND POLICIES 924-31 (3d ed. 2006).

191. *See* N.Y. Times v. Sullivan, 376 U.S. 254, 279-80 (1964).

192. *See* Reno v. ACLU, 521 U.S. 844, 870 (1997) (stating that online, "any person with a phone line can become a town crier with a voice that resonates farther than it could from any soapbox").

193. *See* Siva Vaidhyanathan, *Me, "Person of the Year"? No Thanks*, MSNBC, Dec. 28, 2006, http://www.msnbc.msn.com/id/16371425/ ("Google, for instance, only makes money because it harvests, copies, aggregates, and ranks billions of Web contributions by millions of authors who unknowingly grant Google the right to capitalize, or 'free ride,' on their work.").

194. *See* Eugene Volokh, *Freedom of Speech and Information Privacy: The Troubling Implications of a Right to Stop People from Speaking About You*, 52 STAN. L. REV. 1049, 1074 (2000) (arguing, with respect to the free rider problem, that the fact that companies make money selling information about people without compensating them, "cannot be the justification for restricting speech, unless we are willing to dramatically redefine free speech law.").

195. *See* Lemley, *supra* note 59, at 15; Assaf Hamdani, *Who's Liable for Cyberwrongs?*, 87 CORNELL L. REV. 901, 916-18 (2002) ("ISPs do not capture the full value of the conduct they are entrusted with policing.").

196. Some commentators in fact convincingly argue just the opposite—that Google is offering too many services for free and thereby potentially hindering other online entrants. *See, e.g.*, Tom Foremski, *The Limits of Google's Limitless Business Model*, SILICONVALLEYWATCHER, May 15, 2006, http://www.siliconvalleywatcher.com/mt/archives/2006/05/part_1_the_limi.php; Michael Schrage, *Why Giveaways Are Changing the Rules of Business*, FT.COM, Feb. 6, 2006, http://www.ft.com/cms/s/2/01e4b1a4-

IV. CONCLUSION

Even if they might have applied to Web 1.0, offline analogies and their corresponding liability systems tend to fall short in Web 2.0. Service providers are not like shop-owners, who logically should not face liability for libelous graffiti others put on the walls of their stores. Instead, in Web 2.0, providers sort the graffiti, encourage it, arrange it by category, make money by putting relevant ads next to it, and repackage and redistribute it for display on other shop's walls—instantly. What role § 230 and courts' broad interpretation of it has to this point played in bringing about the staggering growth of the Web and these kinds of services it is not totally clear—certainly it is not simple causation. Nevertheless, both in theory and in practice, as both economic theory and the cases to date demonstrate, the minimal interference scheme set forth in *Zeran* poses no significant hurdles to Web 2.0, in contrast to its alternatives.

9741-11da-82b7-0000779e2340.html (citing Google's bundling of email and other 'free' services and explaining that "[o]ne company's clever cross-subsidy is another's anti-competitive predatory pricing.").