2012

Website Design and Liability

Nancy Kim
California Western School of Law, nsk@cwsl.edu

ARTICLES

WEBSITE DESIGN AND LIABILITY

Nancy S. Kim*

ABSTRACT: Two regrettable behaviors have emerged online: the posting of content about others without their consent; and impulsive postings with no consideration of long-term consequences. Website operators can either encourage or discourage these regrettable behaviors and influence their consequences through the design of their website and by the fostering of norms and codes of conduct. Unfortunately, courts interpret section 230 of the Communications Decency Act as providing websites with broad immunity. In an earlier article, I argued that a proprietorship standard should be imposed upon websites, which would require them to take reasonable measures to prevent foreseeable harm. This article further champions the concept of website proprietorship liability and proposes that section 230 should be amended to recognize such liability with provisions for the following "safe harbors" for website operators that: (1) permit only postings by identified posters; (2) have nonprofit status and do not accept ad revenue; and (3) remove postings upon request of the victim. This article also addresses anticipated objections that are based upon market concerns and free speech concerns.

CITATION: Nancy S. Kim, Website Design and Liability, 52 Jurimetrics J. 383–431 (2012).

This article argues for a comprehensive proposal to amend section 230 of the Communications Decency Act (CDA), which is the controversial legislation that protects online intermediaries from civil liability for content posted by third parties.[1] Many credit this provision of the CDA with fostering Internet growth and the proliferation of sites where ordinary citizens may express their views.[2] Others, however, alarmed by the unlawful nature of some online com-

*Professor, California Western School of Law. An early version of many of the arguments raised in this paper was discussed at the 47 U.S.C. section 230: A 15-Year Retrospective, Santa Clara Law School, Santa Clara, CA, March 4, 2011. The author gratefully acknowledges the many helpful comments from the participants at that conference that informed this paper. Special thanks are owed to Peter Swire for helping to better analyze and reframe this project at an early stage, and to Jacqui Lipton and Eric Goldman for reviewing a draft of this article and providing much appreciated feedback.

1. Communications Decency Act of 1996, 47 U.S.C. § 230 (2006).

2. Cecilia Ziniti, Note, *The Optimal Liability System for Online Service Providers: How Zeran v. America Online Got it Right and Web 2.0 Proves It*, 23 BERKELEY TECH. L.J. 583, 583 (2008) (concluding that section 230 has "truly fostered the last ten years' development of the web."). An online forum on the topic of cyber harassment on a popular legal blog garnered many heated comments about the pros and cons of limiting speech online. *See* Responses to Danielle

munication, have called for legal reform.[3] While the right to free expression applies to Internet discourse, the parameters of that right have not been clearly established. The unique characteristics of online discourse complicate the analysis. One of the achievements of the Internet is that it enables ordinary people to share their views with countless others. Regulations that require prescreening or content moderation may impose too great a burden on websites that may have millions of daily visitors. The popular online bulletin board Craigslist, for example, claims to have over twenty billion page views per month.[4] On the other hand, the very popularity of certain websites means that defamatory or personally intrusive content is viewed by more people, amplifying the harm. The large volume of postings and the ability to remain anonymous may lead some posters to believe they are hidden in the crowd, causing them to act out in offensive or unlawful ways.

Two regrettable online behaviors have emerged within the last decade. The first is the posting of images or information about others without their consent or approval, which are referred to in this article as "third-party postings." The other is the impulsive posting of images or information (about oneself or others) without consideration of context or long-term implications, which for the sake of convenience is referred to as "impulsive posting." The very characteristics of Internet communication that make it appealing (that is, ease of publication and widespread dissemination) also make it unpredictable and potentially harmful given its other characteristics of permanence and irretrievability.[5] This is not to say that these two behaviors—impulsive posting and third-party posting—are regrettable in every instance. One might argue that impulsive postings, such as tweets,[6] can spur dynamic conversations and facilitate important communications and observations. In some cases, third-party posting may be useful as a means of alerting others to harmful or unlawful conduct. But these two behaviors may have negative long-term social consequences, too, such as the stifling of expression.

Citron, *One Month in Jail: The Sentence in the Ravi Case*, CONCURRING OPINIONS (May 21, 2012, 2:07 PM), http://www.concurringopinions.com/archives/2012/05/one-month-in-jail-the-sentence-in-the-ravi-case.html.

3. Brian Leiter, *Cleaning Cyber-Cesspools: Google and Free Speech, in* THE OFFENSIVE INTERNET, 155, 156 (Saul Levmore & Martha C. Nussbaum eds., 2010) (noting that the effect of section 230 has been "to treat cyber-cesspools wholly differently from, for example, newspapers that decide to publish similar material."); Danielle Keats Citron, *Cyber Civil Rights*, 89 B.U. L. REV. 61, 114–25 (2009) (opposing blanket immunity for website operators); Daniel J. Solove, *Speech, Privacy and Reputation on the Internet, in* THE OFFENSIVE INTERNET 15, 23–27 (Saul Levmore & Martha C. Nussbaum eds., 2010) (arguing for reformation of section 230).

4. *Factsheet*, CRAIGSLIST, http://www.craigslist.org/about/factsheet (last updated Mar. 12, 2012).

5. *See* Jeffrey Rosen, *The End of Forgetting*, N.Y. TIMES, July 25, 2010, (Magazine), at 30 (describing the "collective identity crisis" created by the impossibility of completely erasing one's digital past).

6. A *tweet* is a post on the popular microblogging site, Twitter. *See About Twitter*, TWITTER https://twitter.com/about (last visited July 31, 2012).

Online speech is a double-edged sword when it comes to expression because enabling one person to post may mean another person is forced to suppress herself.[7] Let us assume that someone named Jane regularly posts photos from parties that she has attended to her Facebook account. At subsequent parties, other guests may refrain from drinking or dancing, to protect their reputation. Jane's posting activities stifle the enjoyment and expressive activity of other guests.[8]

The free speech versus privacy debate goes to the very heart of what the First Amendment was intended to protect: expression and autonomy.[9] The freedom to live one's life according to one's own beliefs is central to American society. A critical part of enjoying this freedom is the ability to explore and question existing beliefs and ideas and to try out different identities at different stages of one's life. Yet it is this very freedom—to explore new iden-

---

7. The nastiness of online comments may also have a silencing effect on more civilized participants. *See* Taffy Brodesser-Akner, *E Playgrounds Can Get Vicious*, N.Y. TIMES, Apr. 22, 2010, E8 (discussing the "torrent of anonymous maliciousness" and the effect it has on a writer).

8. For a discussion of the complicated issues arising from privacy, autonomy and the power of technology to create new concerns, see Ruth Gavison, *Privacy and the Limits of Law,* 89 YALE L.J. 421 (1980). Gavison writes that the

> identification of technological developments as a major source of new concern may be supported by the fact that modern claims concerning the secrecy and anonymity aspects of privacy have not been accompanied by new claims concerning physical access: technological advances have affected the acquisition, storage, and dissemination of information, but gaining physical access is a process that has not changed much. On the other hand, the increase in the number of people whose profession it is to observe and report, the intensified activity in search of publishable information, and the changes in the equipment that enables such enterprises, make it more likely that events and information will in fact be recorded and published.

Id. at 466. *See also* Anne Wells Branscomb, *Anonymity, Autonomy, and Accountability: Challenges to the First Amendment in Cyberspaces*, 104 YALE L.J. 1639, 1641 (1995) (discussing the issues raised in cyberspace, particularly with respect to the First Amendment, anonymity, autonomy and accountability); Richard A. Epstein, *Privacy, Publication, and the First Amendment: The Dangers of First Amendment Exceptionalism*, 52 STAN. L. REV. 1003, 1004 (2000) ("Doctrinal analysis often requires us to reconcile traditional legal principle with modern technological innovation. Nowhere is this task of reconciliation more daunting than with cyberspace, where the speed and spread of information has been ratcheted up to levels that were unimaginable even a generation ago. And nowhere in cyberspace is it more important to tweak doctrine than on the general legal issue of privacy, which is here defined as the ability of individuals to keep private . . . information about themselves that could provide harmful or embarrassing to them if made public or placed in the wrong hands."). James Grimmelman has discussed the unintended consequences and privacy violations that occur from information posted on Facebook. *See generally* James Grimmelmann, *Saving Facebook*, 94 IOWA L. REV. 1137 (2009) (explaining how Facebook users socialize on the site and misunderstand the risks involved); James Grimmelmann, *Privacy as Product Safety*, 19 WIDENER L.J. 793 (2010) (providing examples of how information posted on Facebook can be misused).

9. *See* ERWIN CHEMERINSKY, CONSTITUTIONAL LAW: PRINCIPLES AND POLICIES 929 (3d ed. 2006) (noting that a "major rationale often expressed for protecting freedom of speech as a fundamental right is that it is an essential aspect of personhood and autonomy."). While I focus on personal expression here, it also refers to political expression. Sean Scott observes, "The conflict that arises between the right of privacy and the First Amendment freedom of the press may not be one of individual versus society." Sean M. Scott, *The Hidden First Amendment Values of Privacy,* 71 WASH. L. REV. 683, 687 (1996). "The private facts tort does protect an individual's interest in personhood or human dignity, it also promotes some of the same values protected by the First Amendment." *Id.*

tities and viewpoints and to take risks—that is threatened by the two regrettable behaviors.[10] As Anupam Chander writes, many adolescents will respond to the Internet's threat to privacy by "modifying either their private behavior—risking youthfulness—or their public behavior—avoiding positions that might lead to embarrassing disclosures."[11]

The Internet has given ordinary individuals the power to harass and destroy the lives of other ordinary individuals and so threatens to fundamentally change the nature of our society. The rhetoric of freedom (especially of speech) is often used by those who choose to defend bullying and unethical behavior, but in a free society, one should be permitted to express oneself in an intimate setting without fear of being harassed, spied upon, or subjected to blackmail. As Anne Branscomb wrote, autonomy or control over one's personal information is the "flip side of freedom of speech": "This freedom not to speak simply protects the right not to have information disclosed without consent or in a manner that may be contrary to one's interests."[12] Unfortunately, as stories proliferate about vengeful ex-partners and perverted stealth shutterbugs, some may react by tamping their naturally expressive selves, even in places and spaces that would typically be considered private. Without knowing whether a potential lover or roommate today may be a vindictive online poster tomorrow, some may keep themselves fully clothed and sexually inhibited even behind closed doors, in rooms darkened to foil imagined hidden cameras. A paranoid fantasy, perhaps. But one created by our culture.[13] Time, too, plays an important role, shifting and often betraying with its passage. A poster may appreciate the swiftness with which her views are disseminated online, but may regret her impulsivity later when her attitude or views change.[14] A teen-

---

10. *See* Julie E. Cohen, *Examined Lives: Informational Privacy and the Subject as Object*, 52 STAN. L. REV. 1373, 1423–35 (2000) (discussing need for autonomy-based approach to data privacy protection); Jacqueline D. Lipton, *"We the Paparazzi": Developing a Privacy Paradigm for Digital Video*, 95 Iowa L. Rev. 919, 982–84 (2009) [hereinafter Lipton, *We the Paparazzi*] (citation omitted) (noting that "the exponential rise of online privacy-destroying technologies has led to increasing concerns about individual privacy in recent years" and that "it is time to consider a new multimodal regulatory approach to protect individual privacy.").

11. Anupam Chander, *Youthful Indiscretion in an Internet Age*, *in* THE OFFENSIVE INTERNET 127 (Saul Levmore & Martha C. Nussbaum eds., 2011). *See also* Lizette Alvarez, *Spring Break Gets Tamer with World Watching Online*, N.Y. TIMES, Mar. 16, 2012, at A10 (reporting that college students on spring break are becoming more reserved out of fear that their antics may show up online).

12. Branscomb, *supra* note 8, at 1644.

13. An article in the *New York Times* noted the increase in delusions relating to reality television or the Internet: "With Internet delusion, patients typically incorporate the Internet into paranoid thoughts, including a fear that the Web is somehow monitoring or controlling their lives, or being used to transmit photographs or other personal information." Sarah Kershaw, *Look Closely, Doctor: See the Camera?*, N.Y. TIMES, Aug. 28, 2008, at G1. While many psychiatrists believe that these patients would be delusional anyways, "the more radical view is that this pushes some people over the threshold; the environment tips them over the edge. And if culture can make people crazy, then we need to look at it." *Id.* (quoting Dr. Joel Gold, who is a clinical assistant professor of psychiatry at New York University) (internal quotation marks omitted).

14. Cautionary tales of online disclosure remorse abound. *See, e.g.*, Emily Gould, *Exposed: What I Gained—and Lost—By Writing About My Intimate Life Online*, N.Y. TIMES, May 25, 2008, (Magazine), at 32.

ager, for example, may enjoy chronicling her exploits online, but may regret divulging such secrets when they prevent her from getting a coveted job later[15] or when they embarrass her future children.[16]

Both behaviors together—impulsive, third-party postings—can be particularly damaging. There are myriad websites that host naked pictures of ex-lovers, reveal secrets and spread lies. The victim has no redress if the website operator refuses to remove the harmful posting. The poster is often anonymous. Even if posters can be identified, they may be judgment proof and a lawsuit, even if successful, would only result in more traffic being directed to the damaging post.[17]

---

15. *See* Jennifer Preston, *Social Medial History Becomes a New Job Hurdle,* N.Y. TIMES, July 21, 2011, at B1 (discussing how information posted on social media sites may impinge a prospective job applicant's chances of getting hired). Information posted online may also affect an applicant's prospects of getting into graduate school. *Id.* In a recent study of 123 top graduate schools of education, engineering, psychology and public administration conducted by Kaplan Test prep, 12% of admissions officers revealed that they were permitted to visit applicants' social networking pages; of those, 29% had rejected an applicant based upon what they discovered. Jacques Steinberg, *The Next Gate,* N.Y. TIMES, July 24, 2011, at ED9.

16. A recent study by the Pew Research Center's reports that one in ten social media profile owners say they have posted content to a social networking site that they later regret sharing. Young adults (15% of profile owners ages 18–29) were considerably more likely to express such regret than profile owners ages 50 and old (5%). PEW INTERNET & AMERICAN LIFE PROJECT, PRIVACY MANAGEMENT ON SOCIAL NETWORKING SITES 11 (2012), *available at* http://pewinternet.org/~/media//Files/Reports/2012/PIP_Privacy_management_on_social_media_sites_022412.pdf. Helen Nissenbaum analyzes the importance of context in private information disclosures more fully. *See* Helen Nissenbaum, *Privacy as Contextual Integrity,* 79 WASH. L. REV. 119 (2004). Nissenbaum argues that contextual integrity should be a benchmark for analyzing privacy intrusions. *Id.* at 138. Under Nissenbaum's theory, "a privacy violation has occurred when either contextual norms of appropriateness or norms of flow have been breached. . . . [P]ersonal information revealed in a particular context is always tagged with that context and never 'up for grabs.'" *Id.* at 143. *See also* Chander, *supra* note 11, at 124–25 ("The Internet Age can place a person's history, or, worse, a fleeting episode from that history, at the world's call. The past might haunt the twenty-first-century child till the end of her days. . . . Decisions in such a life require consideration not only of the reputational consequences via-à-vis families, friends, and acquaintances, but also with respect to future employers, partners, and even unborn children."); Josh Blackman, *Omniveillance, Google, Privacy in Public, and the Right to Your Digital Identity: A Tort for Recording and Disseminating an Individual's Image Over the Internet,* 49 SANTA CLARA L. REV. 313, 343–44 (2009) (stating that "where an image captured of a person engaging in an activity may easily be taken out of context, such a chance to explain the photograph is not a possibility, as the subject might not have even been aware he was recorded.").

17. *See* Nancy S. Kim, *Website Proprietorship and Online Harassment,* 2009 UTAH L. REV. 993, 1008–12 (2009) (outlining the inadequacy of existing legal remedies for online harassment). *See also* David S. Ardia, *Reputation in a Networked World: Revisiting the Social Foundations of Defamation Law,* 45 HARV. C.R.-C.L. L. REV. 261, 261 (2010) (arguing that "defamation law suffers from significant doctrinal and practical limitations that preclude it from achieving its goal of protecting reputation."); Lyrissa Barnett Lidsky, *Silencing John Doe: Defamation & Discourse in Cyberspace,* 49 DUKE L.J. 855, 859 (2000) (citations omitted) (noting that defendants in defamation actions may not have deep pockets and may be unable to satisfy a judgment).

Given the inadequacy of existing legal remedies to address the harm caused by online postings,[18] the best strategy is prevention and deterrence.[19] Website operators are in the best position to prevent and deter harmful online conduct; [20] unfortunately, because they also have broad immunity for content posted by their users, they may have no incentive to do so.[21] In this article, the concept of website proprietorship liability that I proposed in an earlier article is developed further.[22] Part I briefly summarizes the rationale for website proprietorship liability and discusses the advantages of a reasonableness standard.

---

18. The scholarly literature on the challenges that user generated content websites create for privacy law is vast. *See generally* DANIEL J. SOLOVE, THE FUTURE OF REPUTATION: GOSSIP, RUMOR AND PRIVACY ON THE INTERNET (2007) (exploring the implications of user-generated content on the reputation of others); Jacqueline D. Lipton, *Mapping Online Privacy,* 104 NW. U. L. REV. 477, 494–514 (2010) (examining different aspects of privacy to gain a comprehensive view of online privacy); Patricia Sánchez Abril, *Recasting Privacy Torts in a Spaceless World,* 21 HARV. J.L. & TECH. 1 (2008) (analyzing the public disclosure tort and its suitability for online harms).); Jacqueline D. Lipton, *Mapping Online Privacy,* (examining different aspects of privacy to gain a comprehensive view of online privacy); DANIEL J. SOLOVE, THE FUTURE OF REPUTATION: GOSSIP, RUMOR AND PRIVACY ON THE INTERNET (2007) (exploring the implications of user generated content on the reputation of others)

19. As Michael Rustad and Thomas Koenig, state:

> The judiciary's inflated interpretation of § 230 has created a legal environment that is ideal for injury and difficult for redress. ISPs have no obligation to remove tortious materials, to prevent the reposting of objectionable materials, or to help victims track down the primary wrongdoers. . . . Consumers have the right to pursue primary wrongdoers through tort litigation, but this is rarely a realistic option because the typical cybercriminal finds it easy to default by disappearing to an unknown and unknowable foreign venue.

Michael L. Rustad & Thomas H. Koenig, *Rebooting Cybertort Law*, 80 WASH. L. REV. 335, 341 (2005).

20. Douglas Lichtman captures the rationale for imposing liability on intermediaries in some situations. Lichtman states:

> The conventional economic account makes clear that private parties cannot create the optimal liability regime on their own in instances where the party directly responsible for the bad act is beyond the effective reach of the law, or in instances where transaction costs make contract negotiations implausible. The conventional account further stresses that liability should be considered in instances where one party has the ability to deter or detect the bad acts of another, and also where liability can serve to encourage a party to internalize some significant negative externality associated with its activities.

Douglas Lichtman, *Holding Internet Service Providers Accountable,* REGULATION, Winter 2004–2005, at 54, 56. *See also* Rustad & Koenig, *supra* note 19, at 390 (noting that Internet service providers (ISPs) are "typically in the position of the 'least cost avoider' to prevent future harm to Internet users."). *But cf.* Jacqueline D. Lipton, *Combating Cyber-Victimization*, 26 BERKELEY TECH. L.J. 1103, 1117–18 (2011) (noting that "criminal law may be a better option than civil law for redressing many online wrongs" because it "seeks to punish and deter wrongdoing while civil law seeks to provide remedies that make a plaintiff whole.").

21. *See* Ann Bartow, *Internet Defamation as Profit Center: The Monetization of Online Harassment,* 32 HARV. J.L. & GENDER 383, 418 (2009) (noting that section 230 provides no incentive or obligation to remove harassing posts).

22. Kim, *supra* note 17, at 1034–47. While I previously made a distinction between "publicly accessible" and invitation-only websites that require a password, I have disregarded that distinction for this article. *Id.* at 1000–01. The concerns that I had about including invitation-only websites, such as certain social networking sites, are remedied by the safe harbor provisions that I propose in Part III. Furthermore, given the ease with which content can be copied and pasted from one site to another, the potential for harm is significant regardless of where the content was initially posted.

This Part also analyzes section 230 of the CDA, which is the statute that has been interpreted by many courts as giving website operators broad immunity for hosting user content. The blanket treatment of website operators ignores differences among them and explains how both the underlying policy of the statute and its plain language support the recognition of proprietorship liability. Part I also explores the role that terminology plays in muddling the issues surrounding section 230.

Part II proposes an analysis of reasonableness in the context of website proprietorship liability that focuses on website design and culture. Part II explains how website operators can influence user behavior through user interface design and by fostering and encouraging a particular culture. As Jaron Lanier has observed, "the user interface designs that arise from the ideology of the computing cloud make people—all of us—less kind."[23] Some website operators design interfaces to elicit and inflame that unkindness. Both the design of a website and its culture can exacerbate or mitigate the negative consequences of the two regrettable behaviors. This article does not argue that website operators should necessarily discourage either impulsive or third-party postings. Rather, website operators should examine the ways in which their website design and culture encourage and influence these behaviors, and they should respond (and perhaps, reconfigure their sites) accordingly.

Part III introduces the following three "safe harbors" to website proprietorship liability: notice and takedown, identified postings, and nonprofit status with no paid advertising. In essence, a website operator that qualifies for one of these safe harbors would establish *de facto* that it had acted reasonably to prevent foreseeable harm.

Part IV addresses anticipated objections and arguments against my proposal for website proprietorship liability. They are organized into two general categories. The first is based on market concerns. This category of objection argues that cyber harassment is the inevitable consequence of technological and societal changes. To accommodate Internet growth and innovation, this view proposes that we should relinquish supposedly outdated norms, such as privacy, and succumb to the changes that the Internet brings. The second type of argument is based on free speech concerns.

This article concludes that, despite the many legitimate concerns raised by opponents, the positive benefits of imposing liability along with the proposed safe harbors far outweigh the negative consequences.

I. WEBSITE PROPRIETORSHIP LIABILITY AND SECTION 230 OF THE COMMUNICATIONS DECENCY ACT

Websites are not typically viewed as businesses unless they engage in retail transactions. In an earlier article, I proposed that website operators should be treated as "proprietors" because they exercise control over their websites and have the potential to generate revenue from the operation of their

23. JARON LANIER, YOU ARE NOT A GADGET 61 (2010).

website either directly, by selling goods on the site, or indirectly, by selling user information and advertising space or marketing and publicizing other ventures.[24] Website operators also exert legal power over their users through the use of clickwrap agreements and terms of use.[25] They can require user registration, block certain Internet protocol addresses, and remove content. Yet, despite their proprietorship powers, website operators generally are immune from liability for any harm that arises from content posted by a third party under section 230 of the CDA.[26]

A. Definitional Fuzziness and Cyber Mystification

Section 230 of the Communications Decency Act provides as follows:

> (c) Protection for "Good Samaritan" blocking and screening of offensive material
>
> (1) Treatment of publisher or speaker
>
> No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider.
>
> (2) Civil liability
>
> No provider or user of an interactive computer service shall be held liable on account of—
>
> (A) any action voluntarily taken in good faith to restrict access to or availability of material that the provider or user considers to be obscene, lewd, lascivious, filthy, excessively violent, harassing or otherwise objectionable, whether or not such material is constitutionally protected; or
>
> (B) any action taken to enable or make available to information content providers or others the technical means to restrict access to material described in paragraph (1).[27]

The statute does not explain what "treated as the publisher or speaker" means and does not mention immunity at all; yet, courts have construed section 230 to mean that website operators are immune from liability as publishers or distributors for content posted on their websites by third parties so

24. Kim, *supra* note 17, at 1034–35.

25. *Id* at 1034.

26. *See* Carafano v. Metrosplash.com, Inc., 339 F.3d 1119, 1123 (9th Cir. 2003) (noting that doubts should be resolved in favor of immunity); Zeran v. Am. Online, Inc., 129 F.3d 327, 332–333 (4th Cir. 1997) (holding that the CDA immunized interactive computer service provider that hosted message board, even though it refused to remove false statement after notice); Barrett v. Rosenthal, 146 P.3d 510, 529 (Cal. 2006) (noting that section 230 "does not permit Internet service providers or users to be sued as 'distributors.'").

27. The reference to paragraph 1 may be intended to read "(A)." Communications Decency Act of 1996, Pub. L. No. 104-104, 110 Stat. 56, 133 (codified at 47 U.S.C. § 230 et. seq.).

long as the website operators did not contribute to the creation of the content.[28] In other words, section 230 (at least, as interpreted by the majority of courts)[29] treats website operators—not like publishers or even distributors—but like common carriers with no interest or liability in the content they transport.[30] Website operators are similar to other common carriers in that they transport large quantities of material, but there are important differences. Website operators do more than transport information; they are also the destination for that information. The nature of the material being transported is also different from a telephone call or a piece of mail, as it is publicly viewable and easily distributable. The relationship of a traditional carrier to the material it transports is temporary whereas a website's relationship to its material is permanent, its name forever associated with the material. Because website operators not only transport, but also host the material, they have greater control over it. Even search engines that are most similar to traditional carriers have greater control over their material than their physical world counterparts. Because their transportation of material is repeated rather than one-time, they may be able to control subsequent transmissions of harmful material. Furthermore, they have greater control over the information because it can be digitally inspected or monitored.[31]

Without the threat of liability, websites are free to encourage the worst from their users. They may design their websites to capitalize on impulsivity and anonymity, removing architectural restraints (such as registration requirements or review periods) and goading users to write salacious material about others.[32] For example, one gossip website encourages its collegiate users to "Go ahead, tell it like it is . . . always 100% anonymous . . . ."[33] That same website hosted a contest that encouraged users to "think of something controversial" to win prizes:

---

28. *See Carafano*, 339 F.3d at 1123; *Zeran*, 129 F.3d at 327; *Barrett*, 146 P.3d at 529. *See also* Barnes v. Yahoo!, 570 F.3d 1096, 1101 (9th Cir. 2009). *Cf.* David S. Ardia, *Free Speech Savior or Shield for Scoundrels: An Empirical Study of Intermediary Immunity Under Section 230 of the Communications Decency Act*, 43 LOY. L.A. L. REV. 373, 381 (2010) (noting that section 230 "has not been the 'free pass'" that many believe it is). At least one court has found that section 230 precludes treating intermediaries as publishers not just for the purposes of defamation law but "in general." *See Barnes*, 570 F.3d at 1104 (noting that "section 230(c)(1) precludes courts from treating [I]nternet service providers as publishers not just for the purposes of defamation law, with its particular distinction between primary and secondary publishers, but in general. The statute does not mention defamation, and we decline to read the principles of defamation law into it.").

29. Nancy S. Kim, *Imposing Tort Liability on Websites for Cyber Harassment*, 118 YALE L.J. POCKET PART 116–18 (2008) *available at* http://yalelawjournal.org/images/pdfs/732.pdf.

30. Elsewhere, I have argued that a reasonableness standard should be imposed upon website proprietors. *See* Kim, *supra* note 17, at 1012–47. *See also* Kim, *supra* note 29, at 117–18.

31. Kim, *supra* note 17, at 997.

32. Jaron Lanier observes, "Behavior varies considerably from site to site. There are reasonable theories about what brings out the best or worst online behaviors . . . . My opinion, however, is that certain details in the design of the user interface experience of a website are the most important factors." LANIER, *supra* note 23, at 62–63.

33. CAMPUSGOSSIP, http://www.campusgossip.com/ (last visited Aug. 16, 2012).

> THE GOSSIP POST THAT RECEIVES THE MOST VIEWS, AND THE MOST COMMENTS (REAL COMMENTS) TODAY WILL RECEIVE PRIZES FROM CAMPUSGOSSIP.COM! THINK OF SOMETHING CONTROVERSIAL, TELL YOUR FRIENDS IT'S POSTED ON OUR SITE, AND YOU'LL BE SURE TO WIN! WINNERS WILL BE ANNOUNCED TOMORROW AFTERNOON (THURSDAY) ON THIS SAME POST, SO LOOK FOR IT IN THE GOSSIP SECTION UNDER THE "RANDOM" SCHOOL SECTION! TO POST SOME GOSSIP SIMPLY CLICK "POST GOSSIP" ON THE RIGHT HAND SIDE OF THE PAGE![34]

Websites that encourage users to post negative information about others target those who are least likely to consider the long-term implications of their posts such as spurned lovers or college students.[35] Not surprisingly, the targeted user may react by posting material in an emotionally charged state that she may later regret. Unfortunately, current law does not require website operators to remove postings even where requested to do so by the original, repentant poster.[36] Benefitted by increased traffic and protected by section 230 immunity, the website operator has no incentive to respond to the original poster's takedown request.

There is a tendency in conversations about online use to use blanket terms that conflate meanings. For example, the Internet is a network of computers in which the computers are capable of communicating with each other,[37] but the term *Internet* is also commonly used to describe the various websites and activities accessible using this network.[38] The term *website* is also used in a singular way, to describe any site residing at a URL.[39] Yet, websites differ in purpose, size, traffic, resources, and revenue models. At the time the personal computer and the Internet became available to the masses, catchall, mystifying terms such as *cyberspace* and *the Net* reflected the discomfort of the public towards the novelty of the medium and with technology in general. Yet, the imprecise terminology used to describe online activity often leads to imprecise

---

34. *Gossip Comments*, CAMPUSGOSSIP (Sept. 16, 2009, 10:36:52 AM), http://www.campusgossip.com/home-page-6880.html.

35. DONTDATEHIMGIRL, http://www.dontdatehimgirl.com (last visited July 31, 2012); THEDIRTY, http://www.thedirty.com (last visited July 31, 2012).

36. Kim, *supra* note 17, at 993.

37. Raymond Shih Ray Ku, *Open Internet Access and Freedom of Speech: A First Amendment Catch-22,* 75 TUL. L. REV. 87, 93–94 (2000). Section 230(f)(1) defines the term *Internet* as "the international computer network of both Federal and non-Federal interoperable packet switched data networks." *See also* Communications Decency Act of 1996, 47 U.S.C. § 230(f)(1) (2006); LAWRENCE LESSIG, CODE VERSION 2.0 83 (2006) ("The Internet is a medium of communication. People do things 'on' the Internet.").

38. Dan Hunter, *Cyberspace as Place and the Tragedy of the Digital Anticommons*, 91 CALIF. L. REV. 439, 453 (2003) (discussing how "everyone employs physical vocabulary to talk about events, transactions, and systems that exist or occur online.").

39. The *Oxford English Dictionary* defines a website as "a document or a set of linked documents, usually associated with a particular person, organization, or topic, that is held on such a computer system and can be accessed as part of the World Wide Web." *Web site*, OXFORD ENGLISH DICTIONARY (June 2012), http://www.oed.com/view/Entry/253976?redirectedFrom=website#eid.

discussions or policy solutions that are over- or underinclusive. For example, legislation to combat cyber harassment often fails to address certain unlawful behavior or includes within its ambit too much lawful behavior.[40]

Another imprecise term, *interactive computer service provider*, is contained in section 230 itself. Section 230 defines "interactive computer service" provider as "any information service, system or access software provider that provides or enables computer access by multiple users to a computer server, including specifically a service or system that provides access to the Internet and such systems operated or services offered by libraries or educational institutions."[41] Courts have interpreted "interactive computer service provider" to include all intermediaries.[42] Yet, this definition does not distinguish between gossip sites that solicit damaging content, such as Campus Gossip, and Internet service providers (ISPs) like AOL that function more like passive conduits. The range of interactive computer service providers is wide. Some interactive computer service providers merely transport content. Other websites function like publishers and hold themselves out to the public as the place to go to read a particular type of content. Some message boards traffic in gossip and reputation smearing; others in facilitating the buying and selling of goods and services. Yet, courts fail to recognize these distinctions for purposes of determining section 230 immunity.

The definitional fuzziness of section 230 also extends to another subsection. Interactive computer service providers are immune from liability for content posted by another; however, section 230 does not protect website operators for content that the website operator itself posted or created.[43] Under section 230(f)(3), "information content provider" is defined as "any person or entity that is responsible, in whole or in part, for the creation or development of information provided through the Internet or any other interactive computer service." Yet, as the Ninth Circuit noted in *Fair Housing Council of San Fernando v. Roommates.com*, a website operator can be both a service provider and an information content provider, and it can be liable as an information

40. For example, a recent proposed House of Representatives bill states as follows: "(a) Whoever transmits in interstate or foreign commerce any communication, with the intent to coerce, intimidate, harass, or cause substantial emotional distress to a person, using electronic means to support severe, repeated, and hostile behavior, shall be fined under this title or imprisoned not more than two years, or both." Megan Meier Cyberbullying Prevention Act, H.R. 1966, 111th Cong. § 3(a) (2009). The bill, however, does not provide standards or definitions for what constitutes, for example, coercion or intimidation. *Id.* The proposed bill provides for fines and incarceration for violation of the law. *Id.*

41. 47 U.S.C. § 230(f)(2) (2006).

42. *See* Fair Hous. Council of San Fernando Valley v. Roommates.com, L.L.C., 521 F.3d 1157, 1161–63 (9th Cir. 2008) (describing an operator of a website matching landlords and tenants as an "interactive computer services" provider). The Ninth Circuit found that "the most common interactive computer services are websites." *Id.* n.6 at 1162; Carafano v. Metrosplash.com, Inc., 207 F. Supp. 2d 1055, 1065 (C.D. Cal. 2002) (finding that an online dating site is an "interactive computer service").

43. *Roomates.com*, 521 F.3d at 1162 (noting that "grant of immunity" under section 230 applies "only if the interactive computer service provider is not also an 'information content provider'").

content provider "even if the information originated with a user."[44] A website operator can "edit" content without liability, but it cannot "create" or "develop" it, either "in whole or in part" without losing immunity.[45] Not surprisingly, the line between editing and that of developing and creating is often blurred.[46] The Ninth Circuit, for example, distinguished between passive transmitters of information and those who help develop content, but admitted the difficulties with its interpretation of "develop."[47]

B. Civil Liability and Website Proprietorship

In an earlier article, I argued that website operators should be subject to proprietorship liability, meaning that they should take reasonable measures to prevent foreseeable harms.[48] This article clarifies and develops the meaning of proprietorship liability to include all civil liability.[49] Brick-and-mortar businesses are subject to standards of reasonableness in the way they conduct their business, such as being required to take "reasonable measures" to prevent "foreseeable harm."[50] Online businesses should be subject to the same standard of reasonableness, although how that standard is applied (that is, what is considered reasonable business conduct) should differ depending upon the nature of the business.

The imposition of proprietorship liability deters socially harmful business practices and encourages socially beneficial innovation.[51] A reasonableness

---

44. *Id.* at 1165 (citing Batzel v. Smith, 333 F.3d 1018, 1033 (9th Cir. 2003)).

45. *Id.* at 1163 (noting that in passing section 230, "Congress sought to immunize the *removal* of user-generated content, not the *creation* of content").

46. For example, the Ninth Circuit interpreted development as "referring not merely to augmenting the content generally, but to materially contributing to its alleged unlawfulness. In other words, a website helps to develop unlawful content, and thus falls within the exception to section 230, if it contributes materially to the alleged illegality of the conduct." *Id.* at 1167–68.

47. These difficulties include that "the broadest sense of the term 'develop' could include the functions of an ordinary search engine—indeed, just about any function performed by a website." *Id.* at 1167.

48. *See* Kim, *supra* note 17, at 1034–47. As noted earlier, most courts have found that section 230 does not permit civil liability. *See, e.g.*, Doe v. MySpace, 528 F.3d 413, 422 (5th Cir. 2008) (finding that section 230 bars negligence and gross negligence claims).

49. Other scholars have proposed looking to tort law to address online problems. For example, Michael Rustad and Thomas Koenig have proposed imposing a limited duty of care upon websites when they have been given actual notice. *See* Rustad & Koenig, *supra* note 19, at 373. They state that "[w]hen a website realizes that its services have created a condition involving an unreasonable risk of a cybertort, it should also have a duty to mitigate damages. Websites are not necessarily mere pipes or conduits; they also play a role in creating or enabling cybertorts or infringement." James Grimmelmann has analogized product safety with privacy safety on social networking sites such as Facebook. *See* Grimmelmann, *supra* note 8, at 820–21 (noting that, "good product design discourages or prevents particularly hazardous uses" and observes that "consumer expectations pervade products liability." While he does not advocate the direct application of products liability law to online privacy, he suggests that products liability law might help shape online social privacy law. *Id.* at 826–27.

50. RESTATEMENT (SECOND) OF TORTS § 344 (1965).

51. Jacqueline Lipton writes that "traditional Property rights entail significant concurrent obligations or responsibilities imposed on the proprietary owner as an incident of their Property ownership. Historically, Property rights have never been absolute. They have always involved

standard enables courts to address discrepancies in types of businesses without being constrained by rules that will be quickly rendered anachronistic by technology and changes in the business environment. Size matters. Small businesses have different requirements than larger, more established businesses. The nature of the business also matters. The concerns raised by consumer review websites may be very different from those raised by gossip sites. ISPs may have a much harder time prescreening content than lightly trafficked websites. Even gossip sites should not all be lumped together. Gossip sites covering public figures such as celebrities and politicians should be treated differently from those gossip sites featuring college students or other private individuals. A reasonableness standard enables courts to recognize and parse those differences.

Unfortunately, the judicial interpretation of section 230 lumps all online entities together and focuses on whether the website operator had a role in the development of content, which is relevant to the issue of whether it qualifies as a publisher or speaker. The issue of whether a website operator is a publisher or speaker, in turn, is relevant where the cause of action requires a determination of status as a publisher or speaker, for example, in a claim of defamation (although not only in cases of defamation).[52] The publisher-speaker determination is irrelevant where the cause of action is not based upon liability as a publisher or speaker (that is, in cases where liability is based upon status as a distributor or in other civil liability lawsuits.)[53] The language of section 230 avails itself of such an interpretation. Notably, section 230(c)(1) does not mention immunity for intermediaries. The only exculpatory language in all of section 230 is in subsection (c)(2) with respect to efforts to restrict access to objectionable materials. It is not the language of the existing legislation that is problematic but the expansive judicial interpretation and application of 230 immunity.[54]

Contrary to how many courts have interpreted section 230,[55] the plain language of the provision accommodates the recognition of tort liability. The

---

limitations, often in the form of legal duties owed to others." Jacqueline Lipton, *Information Property: Rights and Responsibilities*, 56 FLA. L. REV. 135, 148–49 (2004).

52. *See* Barnes v. Yahoo!, 570 F.3d 1096, 1104 (9th Cir. 2009) (noting that section 230(c)(1) protection extends beyond defamation).

53. Felix Wu makes a similar point in a recent article. He states that "§ 230 applies to claims that attempt to make intermediaries stand in the shoes of original speakers." Felix T. Wu, *Collateral Censorship and the Limits of Intermediary Immunity*, 87 NOTRE DAME L. REV. 293, 342 (2011). Wu argues that "because intermediaries and original speakers have different incentives to speak. . . . applying liability as if they were interchangeable has negative results for speech. . . . But if a cause of action is not trying to treat an intermediary as a speaker . . . then the intermediary's incentives to speak are no longer relevant." *Id.*

54. Rustad and Koenig state that "an activist judiciary . . . has radically expanded § 230 by conferring immunity on distributors." Rustad & Koenig, *supra* note 19, at 371.

55. *See generally* Doe v. MySpace, Inc., 528 F.3d 413, 418–20 (5th Cir. 2008) (declining to recognize "virtual premises" liability); Carafano v. Metrosplash.com, Inc., 339 F.3d 1119 (9th Cir. 2003) (finding no liability for a matchmaking service for information posted by a third party); Zeran v. Am. Online, Inc., 129 F.3d 327 (4th Cir. 1997) (finding broad immunity); Barrett v. Rosenthal, 146 P.3d 510 (Cal. 2006) (finding no liability for posting an e-mail created by a third party).

caption for subsection (c) is "Good Samaritan" blocking and screening of offensive material. While headings should not be conclusive, the caption indicates that Congress intended to protect blocking and screening activities of intermediaries, an observation that both the Seventh and the Ninth Circuits have made in recent opinions.[56] This seems particularly true when considered in context. Subsection (c) was enacted, at least in part, in response to the ruling in *Stratton Oakmont, Inc. v. Prodigy Services Co.*,[57] which found an ISP liable for defamation as a publisher.[58] The court held that because the defendant attempted to screen out offensive materials, it had assumed greater liability than if it had made no screening attempt whatsoever.[59]

Section 230(c)(2) states as follows:

> (2) Civil liability
>
> No provider or user of an interactive computer service shall be held liable on account of—
>
> (A) any action voluntarily taken in good faith to restrict access to or availability of material that the provider or user considers to be obscene, lewd, lascivious, filthy, excessively violent, harassing or otherwise objectionable, whether or not such material is constitutionally protected; or
>
> (B) any action taken to enable or make available to information content providers or others the technical means to restrict access to material described in paragraph (1).[60]

If (c)(2), captioned "civil liability," were intended to immunize ISPs from *all* civil liability (not just liability in connection with good faith efforts to restrict or remove content) that would by definition include civil actions based upon their status as a publisher or speaker. Yet, that interpretation seems flawed in light of the subsection immediately preceding it, section 230(c)(1). This section states:

---

56. *See* Fair Hous. Council of San Fernando Valley v. Roommates.com, L.L.C., 521 F.3d 1157, 1163–64 (9th Cir. 2008) ("[T]he section is titled, 'Protection for "good samaritan" blocking and screening of offensive material' and, as the Seventh Circuit recently held, the substance of section 230(c) can and should be interpreted consistent with its caption.") (citing Chicago Lawyer's Comm. for Civil Rights Under Law, Inc. v. Craigslist, Inc., 519 F.3d 666, 669 (7th Cir. 2008) (quoting Doe v. GTE Corp., 347 F.3d 655 (7th Cir. 2003))).

57. No. 031063/94, 1995 WL 323710 (N.Y. Sup. Ct. May 24, 1995); 141 CONG. REC. H8469-70 (daily ed. Aug. 4, 1995) (statements of Rep. Cox and Rep. Wyden). *See also Roomates.com*, 521 F.3d at 1163.

> Section 230 was prompted by a state court case holding Prodigy responsible for a libelous message posted on one of its financial message boards. . . . Under the reasoning of *Stratton Oakmont*, online service providers that voluntarily filter some messages become liable for all messages transmitted, whereas providers that bury their heads in the sand and ignore problematic posts altogether escape liability. . . . In passing section 230, Congress sought to spare interactive computer services this grim choice by allowing them to perform some editing on user-generated content without thereby becoming liable for all defamatory or otherwise unlawful messages that they didn't edit or delete.

Id.

58. No. 031063/94, 1995 WL 323710 (N.Y. Sup. Ct. May 24, 1995) at *4–5.

59. *Id.*

60. The reference to paragraph 1 may be intended to read "(A)." 47 U.S.C. § 230 et. seq. (2006)).

> (c) Protection for "Good Samaritan" blocking and screening of offensive material
>
> (1) Treatment of publisher or speaker
>
> No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider.

Subsection (e) states that section 230 has no effect on federal criminal law or intellectual property law.[61] Therefore, *if* subsection (c)(2) were intended to immunize intermediaries from *all* civil liability, then section 230(c)(1) (with the caption "Treatment of publisher or speaker") would serve only to protect the ISP in state criminal actions where liability was based upon the provider's status as a publisher or speaker. If this was in fact what Congress intended, it would have said so and have drafted section 230(c)(1) more clearly to indicate its applicability only to state criminal law prosecutions.

Furthermore, if Congress intended section 230(c)(2) to exculpate website operators from *all* civil liability, it would not have carved out an exemption for particular acts, that is, the good faith removal of obscene material. A better interpretation would be that section (c)(1) prohibits claims against an interactive computer service provider, which are based upon its status as a publisher or speaker. Where the civil claim is not based upon its status as a publisher or speaker, the interactive computer service provider is not liable for good faith efforts to remove offensive material or to restrict access to such materials. By implication, the computer service provider may be liable for actions that are not efforts to limit access to offensive materials.

Another subsection, 230(e)(3), captioned "State law," specifically states that "[n]othing in this section shall be construed to prevent any State from enforcing any State law that is consistent with this section. No cause of action may be brought and no liability may be imposed under any State or local law that is inconsistent with this section." But what other state law is there than state criminal law if the ISP has broad immunity in civil actions? Section 230(e)(1) states that section 230 has no effect on federal criminal law. Accordingly, if section 230(e)(3) were intended to include only state *criminal* law, the drafters would have expressly so stated with a caption "State criminal law" rather than the broader "State law."

A better interpretation of section 230(e)(3) would be that the drafters intended to leave intact state laws, both criminal and civil, that did not impose publisher or speaker liability on website operators for content created by third parties. More specifically, a plaintiff could not sue a website operator as the original publisher or speaker for content posted by a third party, but it *could* sue a website operator for its negligence in conducting its business as an intermediary and distributor of content. Under this interpretation of section 230, no change to the statutory language would be necessary to recognize website proprietorship liability.

---

61. 47 U.S.C. § 230(e)(1)–(2).

Some influential courts have already recognized the potential limits of section 230 of the CDA. The Seventh Circuit expressed doubt that the statute should be interpreted to provide website operators with absolute immunity. It referenced one of its previous opinions, *Doe v. GTE Corp.*,[62] in stating "why section 230(c) as a whole cannot be understood as a general prohibition of civil liability for web-site operators and other online content hosts."[63] It hinted that section 230 may not mean broad immunity for all civil liability but only those based upon its status as a publisher or speaker: "[P]erhaps section 230(c)(1) forecloses any liability that depends on deeming the ISP a 'publisher'—defamation law would be a good example of such liability—while permitting the states to regulate ISPs in their capacity as intermediaries."[64]

The Ninth Circuit Court of Appeals also noted the limits of section 230 immunity. In *Fair Housing Council of San Fernando Valley v. Roommates.com, LLC*,[65] it stated that the "Communications Decency Act was not meant to create a lawless no-man's-land on the Internet."[66]It noted that "the substance of section 230(c) can and should be interpreted consistent with its caption," which reads "Protection for 'good samaritan' blocking and screening of offensive material."[67] In a footnote, it observed that holding businesses liable for their own conduct did not seem to be unduly burdensome.[68]

Both the *Roommates* and the *Craigslist* cases suggest that at least the Ninth Circuit and the Seventh Circuit courts recognize limits to section 230 immunity. These limits are based upon the statutory language itself, which states that interactive computer service providers who are not content creators or developers shall not be treated as publishers or speakers. Both courts noted that the caption of section 230(c) references protection for "good samaritan" blocking and screening of offensive material. The Ninth Circuit noted that the exemption from civil liability is with respect to actions taken to restrict access to objectionable content—"not the *creation* of content."[69]

The conferral of section 230 immunity has led to egregious results, which make a mockery of the term *good samaritan* when applied to certain websites. Michael Rustad and Thomas Koenig provide one example:

> The unintended consequence of immunizing all ISPs from tort liability is that this confers an absolute immunity on feral ISPs that harm the public. In *Ramey v. Darkside Productions, Inc.*, an online adult services website published unauthorized sexually explicit photographs of the plaintiff in its Eros Guide, using content supplied by a customer. The court ruled that the porno-

62. Doe v. GTE Corp., 347 F.3d 655 (7th Cir. 2003).

63. Chicago Lawyers' Comm. for Civil Rights Under Law, Inc. v. Craigslist, Inc., 519 F.3d 666, 669 (7th Cir. 2008).

64. *Id.* at 670.

65. 521 F.3d 1157 (9th Cir. 2008).

66. *Id.* at 1164.

67. *Id.* at 1163–64 (citing *Craigslist, Inc.*, 519 F.3d at 669 (quoting Doe v. GTE Corp., 347 F.3d 655 (7th Cir. 2003)) (internal quotation marks omitted)).

68. *Id.* at 1169 n.24.

69. *Id.* at 1163 (noting that "Congress sought to immunize the *removal* of user-generated content, not the *creation* of content.").

> graphic website was immunized from liability for the plaintiff's tort claims . . . . The *Darkside* court described the § 230(c) "immunity as quite robust, adopting a relatively expansive definition of 'interactive computer service' and a relatively restrictive definition of 'information content provider.'" The website compartmentalized its adult entertainment content and even placed a watermark on the unauthorized photographs. Despite these compelling facts, the court ruled that the federal immunity for publishers applied, granted summary judgment in favor of the pornographer, and left the plaintiff with no redress for her injuries.[70]

In determining whether to impose proprietorship liability in a given situation, a court should consider whether the website operator took reasonable measures to prevent foreseeable harm. This is the same standard adopted by courts to determine liability for premises-based businesses.[71] A reasonableness analysis recognizes the variations among businesses. It considers the differences between online and offline businesses and differences among web-based businesses, including the large volume of traffic on some sites, the difficulty of controlling user conduct, and the problems created by anonymity. The benefit of a reasonableness analysis is that it is an evolving standard and thus one that accommodates technological advancements, societal changes, and adaptations to technology. For example, while a particular website may not be a mere conduit or a common carrier, prescreening content may be difficult and may cause undesirable delays.[72] Yet, as the technology improves, it may be more realistic to expect website operators to employ prescreening tools.[73] Furthermore, a website operator's actions in light of the ability to airbrush out an image or the identity of a particular individual should be considered in a reasonableness analysis. Imagine, for example, that a user posts an image of her daughter's ballet class. One of the girls in the class is wearing a light colored leotard that reveals too much of her developing body. The legal guardian of the girl requests that the daughter's image be removed. The website operator can accommodate that request without removing the entire team photo simply by cropping out or blurring the girl's image or by requiring the poster to do so.

---

70. Rustad & Koenig, *supra* note 19, at 374.

71. *See* Exxon Corp. v. Tidwell, 867 S.W.2d 19 (Tex. 1993); Seibert v. Vic Regnier Builders, Inc., 856 P.2d 1332, 1338 (Kan. 1993) Barker v. Wah Low, 19 Cal. App. 3d 710, 714–15 (App. Div. 1971); RESTATEMENT (SECOND) OF TORTS § 344 (1965).

72. As the Seventh Circuit noted, "if postings had to be reviewed before being put online, long delay could make the service much less useful, and if the vetting came only after the material was online the buyers and sellers might already have made their deals." *Craigslist*, 519 F.3d at 669.

73. Rob Frieden, *Invoking and Avoiding the First Amendment: How Internet Service Providers Leverage Their Status as Both Content Creators and Neutral Conduits*, 12 U. PA. J. CONST. L. 1279, 1311 (2010) (stating that "technologies for monitoring, filtering, and inspecting content have substantially improved" from when the CDA was first enacted). Frieden questions whether an "ISP can continue to qualify for safe harbor exemptions based on its lack of ability to monitor and manage content, or assumptions that content management would constitute an unreasonable operational or financial burden on ISPs." *Id.* at 1312.

The imposition of proprietorship liability recognizes the policy objectives of section 230 (to both encourage Internet growth and greater user control over offensive content) and encourages the development and use of the Internet in a socially beneficial manner. The current broad immunity promotes technological development that is lopsided in favor of growth without social responsibility. Website proprietorship liability, on the other hand, conforms to societal expectations of reasonable business practices. Far from being an unduly harsh burden on online businesses,[74] it merely requires them to be accountable for the products and services that they release to the public. Website proprietorship liability would promote the objectives of both section 230[75] and tort law.

II. WEBSITE DESIGN AND CULTURE AND THE TWO REGRETTABLE BEHAVIORS

This Part discusses two regrettable online behaviors. The first is impulsive posting, which is the posting of content without deliberation of the long-term consequences. The second regrettable behavior, third-party posting, is the posting of content about third parties without their consent. Additionally, an explanation is given about how the choices that website operators make regarding site design and site culture can temper or exacerbate the consequences of these two regrettable behaviors.

A. Two Regrettable Online Behaviors

In the past fifteen years or so, an online culture has emerged with two regrettable online behaviors. The lack of barriers to distribution and the speed of digital communication have resulted in impulsive posting of content. Thoughtfulness and deliberateness have taken a back seat to speediness. Trigger happy e-mailers press send first and feel regret later, and seasoned journalists find themselves "scooped" by amateur bloggers who publish rumors and speculation. The pace of communication grows ever more swiftly, via text messaging, Twitter and Facebook. The barriers to publication have disappeared and with them, quality controls, fact checking, and proper grammar and spelling. There is an additional hazard that comes with speed: emotionalism. A rapid reply is often an emotionally charged one, with no counting to ten before

74. I use the term *businesses* in a calculated manner as I propose a safe harbor for nonprofit sites. *See infra* Part III.

75. Section 230(b) states that the "policy of the United States" is as follows:

> (1) to promote the continued development of the Internet and other interactive computer services and other interactive media;
> (2) to preserve the vibrant and competitive free market that presently exists for the Internet and other interactive computer services, unfettered by Federal or State regulation;
> (3) to encourage the development of technologies which maximize user control over what information is received by individuals, families, and schools who use the Internet and other interactive computer services;
> (4) to remove disincentives for the development and utilization of blocking and filtering technologies that empower parents to restrict their children's access to objectionable or inappropriate online material; and
> (5) to ensure vigorous enforcement of Federal criminal laws to deter and punish trafficking in obscenity, stalking, and harassment by means of computer

Communications Decency Act of 1996, 47 U.S.C. § 230(b) (2006).

posting. While there may be benefits to some impulsive postings—such as timeliness and spontaneity and maybe, in some cases, a type of creativity that results from lack of contemplation—those benefits should be considered against the potential harms, especially when combined with the second regrettable behavior.

The second regrettable online behavior is the posting of information about third parties, without their consent. As with impulsive posting, third-party posting can be socially beneficial. The public may be warned about nefarious characters, hazardous products or fraudulent businesses. One can share good news about a friend on a social networking site. But third-party posting can also be very harmful. A malicious poster can reveal secrets and post private images. The ubiquity of cellular phones with cameras can hinder our everyday activities turning, for example, an excursion to the gym into an opportunity for online harassment.[76] Third-party posting, whether well intentioned, strips the subject of a person's autonomy in that she is no longer able to make the decision about whether to share personal information or experiences.

Something combustible often occurs when these two regrettable behaviors coincide. Impulsive posting about third parties can be gossipy, mean, and vengeful. Even when it is simply thoughtless, misguided, and clueless, such postings can cause reputational and emotional harm that cannot be entirely erased. The stakes are high and can affect the subject of the post for years to come. An unflattering post may affect one's job prospects, for example, as more companies use social media to conduct background checks of potential employees.[77] While some may argue that impulsive or third-party posting is not always bad, posts that are the result of thoughtful deliberation are, normatively speaking, almost always better. Society benefits from self-editing. Self-editing is not the same as institutional or governmental censorship. Similarly, garnering consent from third parties before posting information about them is also better as a norm. Unfortunately, these two regrettable behaviors have a way of spreading virally throughout the online culture as users conform to their influence and thus perpetuate them.

As noted in Part I, a determination of reasonableness for purposes of website proprietorship liability should be fact and context based. The reasonableness of measures adopted by a leanly staffed start-up with little traffic should not be compared with the measures adopted by an online giant like Facebook or Google. Website operators affect the way users conduct themselves on a site through website design and the fostering of a particular culture. For example, a website that permits anonymous postings invites greater openness and less formality. Users may also exercise less self-restraint and inhibition. Website operators should be cognizant of the way design interacts with the two regrettable online behaviors. This does not mean that website operators

76. *See* Catherine Saint Louis, *Cellphones Test Strength of Gym Rules*, N.Y. TIMES, Dec. 8, 2011, at E1.

77. Preston, *supra* note 15 (discussing a company that "scrapes the Internet for everything prospective employees may have said or done online in the past seven years."). The information obtained by that company has resulted in job offers being withdrawn. *Id.*

should never permit impulsive or third-party posting; what it does mean is that they should anticipate and implement safeguards to prevent the negative consequences that so frequently accompany them. Part II.B discusses some of these safeguards.

B. Reasonable Proprietorship, Website Design, and Culture

As previously discussed, website operators should take reasonable steps to prevent foreseeable harm. Where the website operator designs its site to facilitate or encourage one or both of the regrettable behaviors, it should anticipate certain bad faith postings by its users. For example, while most websites want more traffic, what they do to increase traffic and what they want from their users differs. A retailer, like Amazon.com, wants to encourage users to buy. A news-oriented website such as the Huffington Post wants users to read content, not only to generate more ad revenue, but also to gain influence over public opinion. Some websites, such as Facebook or YouTube, want their users to create content. But even user generated content sites have different objectives. Facebook wants user generated content so that its members can better communicate with their friends. The objective is to extend and enhance social networks. Accordingly, the traffic generated is to individual user accounts on Facebook. YouTube, on the other hand, wants user-generated content that entertains and draws a broad audience of strangers. Presumably YouTube benefits more from clips that appeal to a large cross section of the population rather than those of interest primarily to the posters and their friends.[78] Facebook intends for user-generated content to strengthen social bonds among friends and acquaintances whereas YouTube wants its user generated content to attract the attention of the masses. On both sites, there is no prescreening of content and users can post content easily. However, both Facebook and YouTube have tempered the negative effects of impulsive postings through the design of their sites. Both sites discourage impulsive postings by requiring registration before uploading content. Registration requires submission of an e-mail address, a username, postal code, date of birth and gender.[79] Even if posters use a pseudonym and are unknown to the general public, they are identifiable by the website unless they take affirmative steps to create a false identity and an associated fake e-mail account. Each required step mitigates the impulsivity norm.

A site's motivations for registration may differ. In a book about the social networking site, MySpace, Julie Angwin explains how the company made a

78. YouTube recently announced plans to create designated channels to highlight more professionally created content. *See* Ian Paul, *YouTube Spending $100M to Compete with Broadcast TV*, PCWORLD (Apr. 7, 2011, 7:53 AM), http://www.pcworld.com/article/224523/youtube_spending_100m_to_compete_with_broadcast_tv.html.

79. *Create a New Google Account*, GOOGLE, https://accounts.google.com/SignUp (last visited Aug. 17, 2012) (YouTube accounts are created through signing up for a Google account.); *Sign Up for Facebook*, FACEBOOK, http://www.facebook.com/r.php (last visited Aug. 17, 2012).

conscious business decision to allow "Fakesters," or members who use fake identities to cultivate an unrefined, irreverent culture.[80]

YouTube requires posters to be registered with the site, but visitors are free to watch videos without registering.[81] YouTube encourages viewers to browse by making it easy to do so, by listing popular videos on its home page, categorizing videos and creating personalized recommendations, and highlighting video trends.[82] YouTube thus designs its website to encourage impulsive *viewing* and tempers the negative consequences of impulsive *posting* with a registration requirement.

Facebook also requires registration to join the site.[83] Postings after registration are intended to be instantaneous and frequent. The design of Facebook encourages impulsivity but the negative consequences of impulsivity are tempered by the nature of the site itself, which discourages anonymity.[84] A member's page can be either open to the public or closed, but the member must be identified to attract viewers. If a member uses a pseudonym, she must still notify others for them to gain access to her Facebook postings. Facebook also has a "safety center" to provide resources to address online safety concerns relating to juvenile users.[85] One safety feature, the social reporting tool, addresses third-party posting. This tool permits a user to directly ask another Facebook member to remove a post or photo, and remove a friend or block an offending poster.[86] The user can also request Facebook to remove the offensive post.[87]

By contrast, gossip sites exploit both regrettable behaviors and specialize in getting users to impulsively post content about others. The gossip site, TheDirty.com, encourages users to "Submit Dirt" via a large button on the home page.[88] Users are not required to register and can either e-mail the website or upload the content directly. The operator of the site adds denigrating comments to posted images of women, thereby encouraging the culture of

---

80. JULIE ANGWIN, STEALING MY SPACE: THE BATTLE TO CONTROL THE MOST POPULAR WEBSITE IN AMERICA 59–63 (2009).

81. YOUTUBE, http://www.youtube.com (last visited Aug. 1, 2012).

82. *Id.*

83. FACEBOOK, http://www.facebook.com (last visited Aug. 1, 2012).

84. Facebook has undergone public criticism because of its efforts to make private information public. *See, e.g.*, Eliot Van Buskirk, *Report: Facebook CEO Mark Zuckerberg Doesn't Believe in Privacy,* WIRED (Apr. 28, 2010), http://www.wired.com/epicenter/2010/04/report-facebook-ceo-mark-zuckerberg-doesnt-believe-in-privacy/.

85. *Family Safety Center*, FACEBOOK, http://www.facebook.com/safety/ (last visited Aug. 1, 2012).

86. Facebook Safety, *Details on Social Reporting*, FACEBOOK (Mar. 10, 2011, 4:09am), http://www.facebook.com/safety/. *See* Larry Magrid, *New Facebook Safety Center Helps, But Safety Remains a Shared Responsibility,* HUFFINGTON POST (Apr. 19, 2011), http://www.huffingtonpost.com/larry-magrid/new-facebook-safety-cente_b_851261.html.

87. *Id.*; *Facebook Community Standards*, FACEBOOK, http://www.facebook.com/community standards (last visited Aug. 1, 2012).

88. THEDIRTY, *supra* note 35.

online stone throwing.[89] Another website, Campusgossip.com, also makes posting content easy, including a button labeled, "Upload and Move On."[90] Posters are not required to register and posting is fast and anonymous or pseudonymous. Just as registration and the possibility of identification encourage accountability, nonregistration encourages impulsivity and a lack of accountability.

The culture established by each website can either mitigate or exacerbate the two regrettable behaviors. A website that purports to help you "connect and share with the people in your life"[91] emphasizes a participatory culture that depends upon the user's identity and reputation, whereas a site that urges users to "submit dirt"[92] with pictures on the home page of scantily clad women fosters a voyeuristic, misogynistic culture where posters and viewers can mock and condemn without fear of their identities being revealed.

Another way that site operators can establish a culture is through their terms of use or "community guidelines."[93] Some sites, for example, forbid the posting of hate speech[94] or sexually explicit content.[95] Other sites tout their status as "gossip and satire" sites and expressly disclaim responsibility for posted information.[96] A site can require a user to read the guidelines before posting, or may impose them in a more passive way, through a link on the site. A site that requires clicking "I agree" to the websites community guidelines before posting may ameliorate some of the negative effects of the two regrettable behaviors by inserting a delay in the posting process and by reminding the poster of behavioral expectations.

Websites that encourage impulsive postings, third-party postings, or both, should expect that some users will upload content that they will later regret and wish to remove. Some websites temper impulsive postings by enabling the user to directly remove previously uploaded content. Facebook, for example, gives users the ability to remove content that they posted. However, other sites do not give users control over their content once it is posted.[97]

Another way that site operators can cultivate a particular culture is by actively monitoring the site for inappropriate content. A website operator can, for example, delete posts that violate its terms of use or guidelines. On the other hand, an operator who wishes to foster a crude and vulgar site might tout its refusal to monitor comments and may disclaim responsibility for content.

---

89. *See* Kevin Engstrom, *The Dirty on TheDirty.com: Founder Claims Woman Trashing Site "Needed" by Society, Above Canadian Law*, WINNIPEG SUN (Apr. 9, 2011), http://www.winnipegsun.com/news/columnists/kevin_engstrom/2011/04/09/17936936.html.

90. *Post a* Pic, CAMPUSGOSSIP, http://www.campusgossip.com/post-a-picture (last visited July 31, 2012).

91. FACEBOOK, *supra* note 83.

92. THEDIRTY, *supra* note 35.

93. *See Community Guidelines*, YOUTUBE, http://www.youtube.com/t/community_guidelines (last visited July 31, 2012).

94. *Id.*

95. *Id.*

96. *Terms of Use*, THEDIRTY, http://thedirty.com/terms-of-use/ (last visited July 31, 2012).

97. *See id.*; RIPOFF REPORT, http://www.ripoffreports.com (last visited July 31, 2012) (*Ripoff Report's* policy is not to remove posts by users under any circumstances.).

1. *A Reasonable Cyber Harassment Policy*

A foreseeable consequence of impulsive and third-party posting is the posting of content that is defamatory or invasive of a third party's privacy. *All* websites that permit user-generated content should anticipate complaints and requests from third parties for removal of content. Accordingly, these website operators should implement harassment policies to address complaints in a timely manner in the same way companies have implemented policies to deter sexual harassment. A cyber harassment policy educates its users, establishes norms of conduct, and raises awareness about the consequences of unacceptable actions. While prescreening may not be feasible in many cases, a website should have standards for internal review of content. Such a policy should be reasonable on its face and have a way of addressing common problems created by the two regrettable behaviors. The rest of this subsection provides examples of situations that should be anticipated by a website operator that permits posting of content by users.

a. Websites Should Take Down Material Upon Request of the Poster

A website operator that permits user generated content on its site should anticipate the occasional remorseful poster, someone who has fallen victim to one or both of the regrettable behaviors and later wishes to retract a post.

Under section 230, a website is not liable for content, even if it is false or otherwise tortious. The original poster, however, is not immune from tort liability. Furthermore, the likelihood of harm (and potential magnitude of damages for which the poster is liable) increases the longer the material remains on the website. The views expressed may no longer reflect those of the poster. A reasonable cyber harassment policy should include taking down material upon request of the poster. The burden on the website's resources is minimal. A takedown request by the original poster does not require onerous prescreening or difficult subjective decisions on the part of the website operator. Posters can be contractually prohibited from requesting more than a specified number of takedown requests and repeat offenders can be banned from the website, thereby limiting the administrative burden of responding to fickle or ambivalent posters. Given the minimal burden upon the website operator, the potential liability of the poster, and the importance of autonomous expression, a reasonable cyber harassment policy should include the removal of posting upon request of the original poster.

b. Websites Should Take Down Unauthorized Nude Images Upon Request of the Subject

Online postings are widely distributable and easily reproducible and nude images have the potential to create devastating harm. In *Barnes v. Yahoo!, Inc.*, the plaintiff sued Yahoo! for failing to remove unauthorized "profiles," which included nude pictures of the plaintiff that had been posted by her ex-boyfriend.[98] The plaintiff's ex-boyfriend posed as the plaintiff in Yahoo!'s

98. Barnes v. Yahoo!, Inc., 570 F.3d 1096, 1098 (9th Cir. 2009).

online chat rooms and directed men to the profiles that he had created.[99] As a result, strangers seeking sex bombarded the plaintiff with e-mails, phone calls and personal visits.[100] Yahoo! failed to remove the profiles for several months, removing them only when the plaintiff filed the lawsuit.[101] The federal district court held that section 230 barred plaintiff's claim.[102] While the Ninth Circuit agreed that section 230 barred the plaintiff's claim "under Oregon law, for negligent provision of services," the court went on to state that the plaintiff may have a claim under a theory of promissory estoppel, which would not be barred by section 230.[103]

A reasonable cyber harassment policy should include a process by which unauthorized nude images are immediately removed upon request of the subject. The *Barnes v. Yahoo!, Inc.* case illustrates the necessity of immediate action when unauthorized nude images are posted online. While a photographer may have an expressive right and a copyright in her photographs, an individual has a personal interest in her image. The website, however, has no rights in images posted by third parties (unless it obtains those rights contractually). If, as alleged, Yahoo! failed to remove the images of the plaintiff within a reasonable time after receiving notice (including receipt of a copy of her photo ID and a signed statement denying her involvement with the fraudulent profiles)[104] from the plaintiff, Yahoo!'s conduct would be unreasonable. On the other hand, if the profiles were removed but were then reposted, the issue of reasonableness would depend upon whether the company was able to block the repostings by, for example, banning the ex-boyfriend from the site.[105]

Unauthorized posting of nude images disproportionately harms those individuals who do not conform to mainstream society views of sexuality. The term *sexuality harassment* is used here to refer to situations where perpetrators single out for ridicule or aggression individuals on the basis of their sexuality. Sexuality's meaning is broad and expansive.[106] I use the term *sexuality* in this article to refer to biological factors as well as societal constructs. It can refer to gender identification, sexual orientation, the sex act itself, or signals and signaling mechanisms to potential sexual partners or society at large. It captures the way individuals talk, dress, walk, and shake their hair. Sexuality thus implicates core issues relating to self-expression, identity, and self-actualization.

---

99. *Id.*

100. *Id.*

101. *Id.* at 1098–99.

102. *Id.* at 1099.

103. *Id.* at 1105–06.

104. *Id.* at 1098–99 (noting that after Barnes requested that Yahoo! remove the unauthorized profiles it allegedly "did not respond.").

105. Yahoo! should also have responded in a timely manner. Instead, the court found that a month after Barnes complained, the company still had not responded. *Id.*

106. *Webster's* dictionary defines *sexuality* as "1. The condition of being characterized by sex. 2. Concern with or interest in sexual activity. 3. The quality of having a sexual character or potency." WEBSTER'S II NEW COLLEGE DICTIONARY 1012 (1995), s.v., "sexuality."

Although highly personal, sexuality extends beyond the individual and is shaped by and reflects political and social dynamics. A boy growing up in a traditional household in a conservative small town may be reluctant to express his sexual interest in other boys. A student at a large university in a cosmopolitan city may conceal her lack of sexual experience. A man may hide his desire to wear women's underwear. In other words, sexuality harassment reflects a societal judgment or normative bias against a particular expression of sexuality. In fact, it is societal approbation that characterizes and distinguishes sexuality harassment.[107]

Unfortunate sexual stereotypes and harsh societal realities make the consequences of unauthorized nude postings different depending upon the subject.[108] To make generalizations can be dangerous, but consider the *Barnes v. Yahoo!, Inc.* case with roles reversed. It would be difficult to imagine a scenario where a woman posts a nude picture of her ex-boyfriend, which results in women appearing at his doorstep to have sex with *him*.[109] Harassment often depends upon social norms and mores so that the perceptions of the victim are considered in light of how closely they align with society's views of the acceptability of the poster's actions. If, for example, someone posts an image of a woman with the comment, "What a beautiful woman!" the actions of the poster ordinarily would not be considered harassment even if the individual perceived the actions as demeaning. In other words, the characterization of an action as harassment often depends upon society's judgment of the action.

Similarly, the *consequences* of a harassing post are determined by society's judgment of the depicted act. If the victim's sexuality, as depicted in the posting, does not conform to mainstream or majoritarian social norms, the consequences are much more severe for the victim. The victim may suffer ridicule, ostracism, and acts of physical aggression. In other words, the act must be viewed in societal context. Sexuality harassment is often directed toward women who do not conform to a certain narrow and constructed version of female sexuality. The founder of one gossip website claims that he is providing a service by holding the women posted on his website accountable for their actions.[110] Postings on that site tend to malign women for their sexual behavior, the way they dress or for not conforming to certain physical expectations. One posting attacked a woman for "clubbing" and claimed that "she's now spreading her legs to any guy she meet's [sic] at the bars" and "spreading

---

107. Although sexuality harassment occurs offline, this article specifically refers to online sexuality harassment to distinguish it from sexual harassment in the context of employment.

108. Chander observes that "[t]he problem of intrusions with respect to sexual privacy may be more grave for women than men, for at least two reasons. First, society has long allowed men greater latitude in sexual affairs than it affords women. . . . Second, women are more likely to be the subject of nude photographs." Chander, *supra* note 11, at 129.

109. Danielle Keats Citron notes that the harassment of women online is a "pernicious and widespread problem" and has a "profound effect on targeted women" that causes significant harm. *See* Danielle Keats Citron, *Law's Expressive Value in Combating Cyber Gender Harassment,* 108 MICH. L. REV. 373, 374–75 (2009).

110. *See* Engstrom, *supra* note 89.

her legs like the slut she is."[111] The online stone throwing continues in the comments with statements such as "[I] hate this bitch!"[112] "Is this a man or a woman? Can't tell the difference."[113] And "E.T. go home your [sic] dirty trash bag!"[114] And "this one is a major dirty whoremaster!!!"[115] Another user posted photos of a woman, calling her the "most disgusting girl in the state of Kansas" and a "fat cow."[116] On one section of the site, posters upload photos seeking the website operator's opinion on the subject women, which is almost always negative. For example, under one posted photo, the website operator comments that a woman's "inner thighs clap, she has some extra muscles below her pits which she only photoshopped on one side of the bottom pic . . . that's also not her hip she's holding onto, its [sic] an over-sized muffin top."[117]

One possible, albeit incomplete, solution to online sexuality harassment is to mandate that images of nude individuals that have been posted without the authorization of the subjects be removed upon their request. In response to concerns about vagueness, nudity should be defined as images of an individual's genitalia or buttocks, and images of a female subject's breasts, where the subject individual is identifiable. Such images are likely to be invasive of privacy.[118] Even where the subjects consented to the taking of the photographs in a particular context, they may not have consented to the online posting of the photographs.[119]

As an example, someone may consent to the taking of nude pictures within the context of a relationship. After the relationship ends, a vindictive ex-lover may post the photograph online as an act of revenge. Ann Bartow notes that amateur pornography may include "fairly transparently an effort to disgrace or damage the subject of the pornography. 'Revenge' pornography appears to be a widespread phenomenon, very popular with pornography viewers attracted by the eroticization of acts of targeted personal humilia-

---

111. *Winnipeg's Trashiest Sloot*, THEDIRTY (Mar. 22, 2011), http://thedirty.com/2011/03/winnipegs-trashiest-sloot. From the comments, it seems as the posting was fabricated by someone who had a dispute with the victim of the post over money: "haha stop posting these Karolina . . . I can't believe you have the nerve to call Jill a slut and whore but now a thief! Lol she is lucky to have money something that you haver [sic] ZERO of which I why you stole from her!! There is a police report for theft against Karolina from her landlord that she stole from as Well as Jill. Jill! love you babe and please do something about this bitch screwing with your life she needs to stop now." Anonymous, *Winnipeg's Trashiest Sloot*, THEDIRTY (Mar. 23, 2011, 10:57 AM).

112. Anonymous, *Winnipeg's Trashiest Sloot*, THEDIRTY (Apr. 8, 2011, 10:51 AM).

113. A.N., *Winnipeg's Trashiest Sloot*, THEDIRTY (Mar. 22, 2011, 9:12 AM).

114. Anonymous, *Winnipeg's Trashiest Sloot*, THEDIRTY (Mar. 22, 2011, 12:36 PM).

115. Anonymous, *Winnipeg's Trashiest Sloot*, THEDIRTY (May 2, 2011, 8:28 PM).

116. Anonymous, *Fat Cow Alert*, THEDIRTY, http://thedirty.com/2011/02/fat-cow-alert-3/ (last visited Aug. 29, 2012).

117. Anonymous, *Would You?*, THEDIRTY, http://thedirty.com/category/would-you/ (last visited Aug. 29, 2012).

118. There are generally four types of privacy torts: (1) intrusion upon the plaintiff's seclusion or into his private affairs, (2) public disclosure of embarrassing private facts about the plaintiff, (3) publicity that places the plaintiff in a false light, and (4) appropriation for the defendant's advance of the plaintiff's name or likeness. William L. Prosser, *Privacy*, 48 CALIF. L. REV. 383, 389 (1960).

119. *See* Nissenbaum, *supra* note 16, at 138 (arguing that the "benchmark of privacy is contextual integrity").

tion."[120] Even if taken in a public place, the nudity may have been highly context specific, such as at a nude beach or campground. Given the highly personal nature of such photographs, immediate removal upon request of the subject is warranted.[121]

The takedown policy regarding nude images should apply even where the subject is a public figure. For example, former Congressman Anthony Weiner was the subject of a highly publicized scandal when he inadvertently publicly distributed a lewd photograph of himself, via Twitter. Subsequently, a blogger released another image, this one of Weiner's penis, which the Congressman had e-mailed to a woman with whom he had been corresponding. The image was distributed on the Internet and eventually resulted in Weiner's resignation. While the initial image was newsworthy, the publication of the image of Weiner's erect penis crosses the line of decency and the public's "need to know." There is no justifiable reason for its release online. As indiscriminate as Weiner might have been about shooting and sending digital images from his computer, he clearly never intended the public to see a body part that is clearly private. Weiner's online activity may be news, but the actual photograph of his penis should not be. While written descriptions of nude images are likely reasonable and legal, the actual image of a man's erect penis in this context is simply pornographic and exploitative. Even public figures should be able to maintain a shred of privacy.

c. Websites Should Take Down Unauthorized Images of Minors Upon Request of Legal Guardian.

While many images of nonpublic figure minors are not as invasive of privacy as nude images, a reasonable cyber harassment policy should include the removal of images of identifiable minors upon request of their legal guardian. Minors are more impulsive and prone to peer pressure. They may post suggestive or revealing images without fully realizing the harmful effects of posting said images.[122] A picture of a minor in underwear or a bathing suit, for example, may attract the attention of sexual predators or the ridicule of peers. Studies indicate that the impulsivity exhibited by teenagers has a biological basis.[123] In an article reviewing some of these recent studies, Dr. Sarah-Jane Blakemore noted that one study suggests that "both emotion processing

120. Ann Bartow, *Pornography, Coercion, and Copyright Law 2.0*, 10 VAND. J. ENT. & TECH. L. 799, 813 (2008).

121. *See* Matthew R. Porio, *Off-Guard and Online: The Unwitting Video Stars of the Web and the Public Disclosure Tort*, 18 SETON HALL J. SPORTS & ENT. L. 339, 367 (2008) (discussing an online video of a college student catching his roommate masturbating).

122. Recent studies indicate that adolescents may not fully comprehend how personal information can be used in unintended ways. For a summary of the recent literature in this area, see Alice E. Marwick et al., *Youth Privacy and Reputation* (Harvard Law Sch. Pub. Law & Legal Theory Working Paper Series, Paper No. 10-29, 2010), *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1588163.

123. *See generally* Sarah-Jayne Blakemore, *Development of the Social Brain During Adolescence*, 61 Q.J. EXPERIMENTAL PSYCHOL. 40 (2008) (summarizing recent studies investigating social cognitive development during adolescence).

and cognitive appraisal systems develop during adolescence."[124] Another study suggests that certain neural changes occur during adolescence that may affect decision making.[125]

Given their peer group, it is not surprising that minors are more likely to be the subject of cyberbullying. Children have created false Facebook profiles and sent e-mails and texts masquerading as their classmates. One mother, for example, reported finding a Facebook page with a photo of her son, along with comments harassing his classmates.[126] After investigating the matter, she discovered that several of her son's classmates had created a false account in her son's name and used misappropriated photos.[127]

A child may become the victim of cyberbullying merely for expressing himself privately.[128] In one well-known example, a teenage boy recorded himself on video wielding a golf ball retriever like a warrior from a *Star Wars* movie.[129] The video was discovered by his high school classmates who posted it to a file sharing website. The video spread virally and was viewed millions of times.[130] Even today, several years after the video was first disseminated, videos of the "Star Wars Kid" may be easily found online, accompanied by hostile and abusive remarks. A recent visit to YouTube, found the following comments: "fat fucking virgin," "asshole," "I think he's mentally retarded," "lol wtf was that faget [sic]," "you look like an [sic] fat dancer ho [sic] has dislexia [sic]," and "this video makes me want to kick this kids [sic] ass. Seriously."[131] This boy's private act of expression became the object of global scorn and ridicule (as well as near-criminal misspellings and cheap psychoanalysis).[132]

While any sentient human being would find this type of abuse unpleasant, children and adolescents are at a critical period of social and emotional development. Minors do not yet have the maturity or the social experience to con-

---

124. *Id.* at 46.

125. *Id.* "[T]he neural strategy for thinking about intentions changes between adolescence and adulthood. Although the same neural network is active, the relative roles of the different areas change, with activity moving from anterior (medial prefrontal) regions to posterior (temporal) regions with age." *Id.*

126. Jan Hoffman, *As Bullies Go Digital, Parents Play Catch-Up*, N.Y. TIMES, Dec. 5, 2010, at A1.

127. *Id.*

128. ENHANCING CHILD SAFETY AND ONLINE TECHNOLOGIES, FINAL REPORT OF THE INTERNET SAFETY TECHNICAL TASK FORCE 4 (2008), *available at* http://cyber.law.harvard.edu/sites/cyber.law.harvard.edu/files/ISTTF_Final_Report-Executive_Summary.pdf (reporting that cyberbullying is a greater threat to teens than sexual predation).

129. Jessica Bennett, *The Flip Side of Internet Fame; In an Age of Google and YouTube, Public Shaming Can Turn Anybody into a Celebrity—or a Fool*, NEWSWEEK (Feb. 21, 2008, 7:00pm), http://www.thedailybeast.com/newsweek/2008/02/21/the-flip-side-of-internet-fame.html.

130. *Id.*

131. *Star Wars Kid*, YOUTUBE (Jan. 15, 2006), http://www.youtube.com/watch?v=HPPj6viIBmU. These postings are a sampling of the many visible on Aug. 29, 2012.

132. According to a lawsuit filed against the classmates who posted the video, the video "may cause [the boy] to be labeled as 'mentally ill' and the stigma could make it difficult for him to enroll in school or get a job, and may force him to change his name." *Star Wars Kid Files Lawsuit*, WIRED NEWS REPORT (July 24, 2003), http://www.wired.com/culture/lifestyle/news/2003/07/59757.

textualize public humiliation.[133] The "Star Wars kid," for example, dropped out of school and enrolled in a children's psychiatric ward.[134]

Furthermore, minors have not yet developed a professional reputation to offset or counter the effect of embarrassing or otherwise negative posted images, which may hinder their future career opportunities.[135] Some critics may charge that websites will be barraged with overprotective parents seeking removal of harmless photographs of their children. It's more likely that parents will complain only if they feel that the images of their children are being misused, which they often are in disturbing ways.[136] A researcher, for example, reports that an image of one child's head was put on a pornographic picture depicting a sexual act.[137] Many of that child's classmates were directed to the online image.[138]

Furthermore, a "takedown-upon-notice" regime might prevent more aggressive action. Recently, a couple called the police to have a man arrested for posting a video of their eight-year-old son spewing profanity.[139] While the man claimed that he would have removed the clip if the parents had asked, it is understandable why the parents might not have been anxious to interact with a neighbor whom they felt compromised the morals of their son by allegedly encouraging him to swear for $1 and then posting the video online.[140] (The man denied both encouraging the boy to swear and paying the boy money).[141] Given the impossibility of ubiquitous parental supervision and lack of control over the taking of digital images of their children, the powerlessness of children to prevent adults from taking their picture, and the substantial interest that parents have in the safety and well being of their children, websites should defer to parental judgment.[142]

---

133. *See supra* notes 27–30 and accompanying text. Ted Brodheim, the chief information officer for the New York City Department of Education, observed, "I don't think they [high school students] fully grasp that when they make some of these decisions, it's not something they can pull back from." Stephanie Clifford, *Teaching About the Web, and Its Troublesome Parts*, N.Y. TIMES, Apr. 10, 2010, at A15.

134. Samuel Axon, *"The Star Wars Kid": Where Is He Now?*, MASHABLE ENTERTAINMENT (June 3, 2010), http://mashable.com/2010/06/03/star-wars-kid/. The "Star Wars kid" is currently a law student and president of a nonprofit dedicated to preserving the heritage and culture of a French Canadian town. *Id.*

135. The poster's reputation may be negatively affected, too if her identity is revealed.

136. For a discussion of the controversy surrounding online posting of children's photographs, see Douglas Quenquo, *Guardians of Their Smiles*, N.Y. TIMES, Oct. 25, 2009, at ST1.

137. Paul J. Fink, *The Case of a Teenager Who Committed Suicide After Being Bullied Online Shows that the Internet Can Be a Weapon Against the Psychiatrically Vulnerable. What Can We Do to Help These Patients?*, CLINICAL PSYCHIATRY NEWS (Feb. 1, 2008), http://www.clinicalpsychiatrynews.com/index.php?id=2407&cHash=071010&tx_ttnews[tt_news]=38523.

138. *Id.*

139. Everton Bailey, Jr., *YouTube Star's Mother Didn't Find Video Funny*, COLUMBUS DISPATCH (Aug. 27, 2010) http://www.dispatch.com/live/content/national_world/stories/2010/08/27/youtube-stars-mother-didnt-find-video-funny.html?sid=101.

140. *Id.*

141. *Id.*

142. *See also* Chander, *supra* note 11, 124–39 (discussing why a reinvigorated privacy tort is necessary to protect youthful indiscretion). Chander's thoughtful essay explains why the Internet

d. Websites Should (Usually) Take Down Private Communication Upon Request of the Writer

The third-party posting behavior has resulted in an unfortunate but common scenario where communications intended to be private are instead forwarded or posted without the writer's consent. A website that permits users to post content should be prepared to address what to do when a user posts private communication from a third party. E-mails are often written quickly and have a different style and purpose than communications intended for a general audience. Furthermore, e-mail communications are typically written using a language, style and references that have meaning only within the contextual framework of a preexisting relationship between the sender and the receiver. A study by the Pew Research Center found that the most common type of cyberbullying among teenagers was the forwarding or public posting of private communication without permission.[143] Nearly 1 in 6 teens reported having had someone forward or post private communication.[144]

In some cases, an intermediary may believe that the public posting of private communication serves a valid public purpose. In that case, the website operator's actions should be subject to a reasonableness analysis. In other words, a decision by the website operator *not* to remove private third-party communications does not necessarily mean that the website operator has acted in an unreasonable or tortious manner. It does mean that the third party may be able to pursue a tort or copyright action against the website operator. It does not mean that the third party will prevail. Furthermore, the possibility of a lawsuit by a third party is mitigated by the availability of the safe harbors set forth in Part III.

e. A Website's Cyber Harassment Policy Must Implement a Reasonable Review Policy

Finally, a cyber harassment policy should have a reasonable review process in place. Any site that permits user-generated content should expect takedown requests and should be prepared to deal with them. A review process does not mean that the website operator must comply with the takedown request, only that the review process should be timely and reasonable. One website allegedly entertains takedown requests with the intent of publicizing them for ridicule or "lulz."[145] That, of course, would not constitute a reasonable review process.

---

and online disclosures threaten to force children to live their lives "as if in a fishbowl," which may lead to youth adopting the "unfortunate strategies" of "excessive caution or foolhardy fearlessness." *Id.* at 124–25.

143. AMANDA LENHART, PEW INTERNET & AMERICAN LIFE PROJECT, CYBERBULLYING AND ONLINE TEENS 2 (2007), *available at* http://pewinternet.org/~/media//Files/Reports/2007/PIP%20Cyberbullying%20Memo.pdf.pdf. The survey was based on responses from 935 teenagers. *Id.*

144. *Id.*

145. *Lulz* is a term that refers to the gratification of causing suffering to others through online activity. *See* LANIER, *supra* note 23, at 61 ("The culture of sadism online has its own vocabulary and has gone mainstream. The common term 'lulz,' for instance, refers to the gratification of watching others suffer over the cloud.") *Id. See also* Mattathias Schwartz, *The Trolls*

Some websites exploit web design and section 230 immunity, appealing to its audience's worst instincts. Gossip and voyeurism generate traffic and increase visibility, which may lead to more advertising revenue or notoriety that a website operator can parlay into other revenue generating opportunities.[146] On the other hand, many websites strive for a broad user base and a more congenial environment. Under a website proprietorship standard, courts would be able to make distinctions between and among different types of websites.

III. LIABILITY SAFE HARBORS

This article advocates the imposition of website proprietorship liability primarily because websites are generally in the best position to respond to harmful postings. Website operators are usually the only parties technically able to remove posts. Because postings are often anonymous, the victim of a harmful post may not be able to seek redress from the poster. Websites have the ability to profit from traffic on their site. Throughout this article, the terms *businesses* and *proprietors* are used deliberately in describing website operators. Website operators have the option of profiting financially from their websites. More page views and a larger user base mean the potential for greater advertising revenue.

Yet, there are some instances where imposing website proprietorship liability on a website operator may be unfair or unwarranted. The threat of liability may stifle fledgling businesses. Some businesses may serve as quasi-public forums and enable users to virtually gather and discuss newsworthy issues. Given the lack of public forums on the Internet, these websites serve a socially beneficial function. The threat of liability may cause these quasi-public forums to disappear.

There are two primary arguments in favor of retaining section 230 immunity. The first is that it encourages innovation, economic growth, and the flourishing of the Internet. The second argument is that it protects free speech online. Both types of arguments are discussed more fully in Part IV.

While a social harm does not always justify a remedy that removes or diminishes associated benefits, neither does a social benefit justify resultant or associated social harms. This article proposes that one way to balance the benefits of section 230 with its burdens is to impose proprietorship liability yet create safe harbors. As discussed in Part I.A., courts should interpret the language of section 230 to permit website proprietorship liability. Unfortunately, they have not. Given that the language of section 230(c)(1) regarding the treatment of websites as "publisher or speaker" has only generated confusion

---

Among Us, N.Y. TIMES, Aug. 3, 2008, at MM24 (Lulz means "the joy of disrupting another's emotional equilibrium.").

146. The use of images to increase traffic may create a right of publicity claim on the part of the individual whose image has been misappropriated. *See* Roberta Rosenthal Kwall, *A Perspective on Human Dignity, the First Amendment, and the Right of Publicity*, 50 B.C. L. REV. 1345, 1345–46 (2009) (noting that the "right of publicity is a legal theory that enables individuals to protect themselves from unauthorized, commercial appropriations of their personas," but the "reality is that many actions based on the unauthorized use of personas involve both dignity and economic harms").

and provides little guidance, this article proposes eliminating this terminology and replacing it with safe harbor provisions that balance the benefits and burdens of proprietorship liability. A website operator that falls under any one of these safe harbors would be deemed to have acted "reasonably." These safe harbors would effectively immunize a website operator from proprietorship liability. Part III.D proposes legislative language to amend section 230 to reflect both proprietorship liability and the safe harbors.

A. Identified Postings and Takedown Compliance

Websites that require that all posting be by identified users would fall under a safe harbor. Posters would put their real name alongside the post and their contact information would be kept on file with the website. Many of the problems of online discourse stem from the lack of ownership of posted content. Postings are often made anonymous or pseudonymously. Jaron Lanier calls "effortless, consequence-free, transient anonymity"[147] or "drive-by anonymity"[148] an important design feature of a "troll-evoking" website.[149]

There are undoubtedly benefits to anonymity. Yet, these benefits must be carefully weighed against the harms that are currently being done by the many who exploit the privilege of anonymity. In a recent letter to the editor of the *New York Times*, Catherine Crump of the American Civil Liberties Union argued for the preservation of online anonymity by urging: "[T]hink about your younger self, and whether you'd want everything you said as a teenager to be permanently linked to your real name."[150] Yet, the names of many children and young adults *are* being permanently linked to posts written by anonymous others, who are free to say what they want about others without revealing their own identities.

These anonymous posters are often goaded by websites that encourage the two regrettable behaviors. As noted in Part II, some websites tout the ease with which postings may be made by unidentified sources, inciting defamatory or malicious postings. Even those sites that require registration before posting typically do not identify the user but maintain the user's registration information solely for their own internal marketing purposes. Without responsibility for content, posters and intermediaries abandon discretion. Victims are left without recourse because posters may be difficult to identify and locate, and intermediaries are immune under section 230. A policy of requiring posters to be publicly identified with their postings may reduce the incidence of both impulsive and third-party posting, and their negative consequences. One notable company has already recognized the potential benefits of identified postings in fostering a desirable culture.[151] The new social networking site,

147. LANIER, *supra* note 23, at 63.

148. *Id.*

149. *Id.*

150. Catherine Crump, Letter to the Editor, N.Y. TIMES (Nov. 26, 2011), http://www.nytimes.com/2011/11/27/opinion/sunday/sunday-dialogue-anonymity-and-incivility-on-the-internet.html?pagewanted=all.

151. GOOGLE+, http://www.google.com/+ (last visited Aug. 16, 2012).

Google+, requires the use of "real names."[152] The "real names" policy, which does not mean legal names, requires that users employ common names or names that they use in everyday life on their Google+ profile.[153] Google's stated reason for this policy is to have a "nicer, more personal, community."[154]

Currently, an anonymous poster can publicly ruin a victim's reputation with no association whatsoever with the act. Identified postings would associate posters with the nature of their postings, thus more closely mirroring the consequences of spreading gossip in the offline world.[155] The posting may lose credibility depending upon the reliability of the poster. Furthermore, the poster, not just the subject of the post, would suffer from a malicious post.

For example, an individual who posts intimate photographs or information about a former lover becomes associated with the act of betrayal, thereby diminishing her chances at future relationships. An increase in the social consequences of spreading harmful information might deter would-be malicious posters as well as provide an alternative to the legal system. As previously noted, the legal system with its focus on remedying rather than preventing harms, often leaves victims of online harassment without a satisfying remedy. Identified postings may enable the victim to bypass the legal system by using social pressure to persuade the poster to remove an offensive post. Thus, the victim would have the option of pursuing a civil action directly against the poster or of using social pressure to persuade the poster to seek removal of the harmful content.

It may be difficult for website operators to verify that a given name and contact information is genuine. The standard for verifying real names should be the listing of a first and last name and the retention by the website operator of contact information. In the event that a complaining party discovers that the given name and contact information of a poster is fake, the website operator must remove the posting if it is to continue to avail itself of this safe harbor. If the website operator removes the posting after discovery that the identity is false, it is immune from liability.

Furthermore, to qualify for this safe harbor, the website operator claiming immunity must promptly remove any content upon request by the original poster. Any expressive interest that the website operator might have in content posted by another should be subordinate to the interests of the poster, especially given that section 230 relieves the website operator from liability. Unfortunately, some website operators exploit section 230 immunity and take advantage of the two unfortunate behaviors by refusing to remove content

---

152. Rob D. Young, *Google+ Takes No-Nonsense Policy on User Identity & Community Standards*, SEARCH ENGINE WATCH (July 22, 2011), http://searchenginewatch.com/article/2095939/Google-Takes-No-Nonsense-Policy-on-User-Identity-Community-Standards (discussing Google's policy on its Google+ network of banning accounts that seem to be using fake names).

153. *Id.*

154. Robert Scobel, *I Talked with Google VP*, GOOGLE+ (July 25, 2011), https://plus.google.com/111091089527727420853/posts/Fddn6rV8mBX#111091089527727420853/posts/Fddn6rV8mBX.

155. Daniel Solove notes that, by gossiping, a person may risk harm to her own reputation. SOLOVE, *supra* note 18, at 140–42.

even where requested by the poster. For example, one consumer review website claims that it provides "a service to the world's consumers."[156] This website, *Ripoff Report*, states that it helps consumers "exercise your first amendment right to freedom of speech. By using our forum, you will have an opportunity to speak out against companies, businesses, government and individuals that have treated you unfairly."[157] It notes, however, that it will not remove posts by users "even if the original author asks us to do so."[158] Yet, on at the bottom of the web page, this same website notes that "it wants to be clear that it accepts no liability for the speech of its users"[159] and that the CDA prohibits a defamed subject "from holding us liable for the statements which others have written."[160] It throws its posters under the bus, adding, "You can always sue the author if you want, but you can't sue Ripoff Report just because we provide a forum for speech."[161]

While one could make a strong argument that a company that seeks to provide a forum for the benefit of the public should have limited immunity, it would not qualify for this particular safe harbor.[162] A website's policy that absolutely refuses to remove content upon poster request fails to consider the realities of the two unfortunate behaviors, and ignores that a user may post in an emotional state that she later regrets. It also disempowers the poster and strips the value of autonomous decision making from the act of expression. Finally, it leaves the poster vulnerable to lawsuits. The website shares none of the responsibility for the post yet maintains total control over its continued publication, exacerbating harms for which the poster may ultimately be liable.

B. Takedown upon Notice-Right of Reply and Poster Identification

A website operator that receives a notice requesting the removal of content would be exempt from liability if it promptly complies with the request. A notice and takedown regime under section 230 would be consistent with other regulatory regimes, such as the Directive issued by the European Parliament,[163] and the Digital Millennium Copyright Act (DMCA),[164] and has been proposed by other critics of section 230.[165] Daniel Solove, for example, proposes that section 230 be modified so that

156. *Frequently Asked Questions*, RIPOFF REPORT, http://www.ripoffreport.com/faq.aspx (last visited Aug. 13, 2012).

157. *Id.*

158. *About Us: Want to Sue Ripoff Report?*, RIPOFF REPORT, http://www.ripoffreport.com/ConsumersSayThankYou/WantToSueRipoffReport.aspx (last visited July 31, 2012).

159. *Id.*

160. *Id.*

161. *Id.*

162. It may, however, fall under the "nonprofit" safe harbor discussed in Part III.

163. *See* Council Directive 2000/31/EC, art. 14–15, 2000 O.J. (L 178); *see generally* THIBAULT VERBIEST ET AL., STUDY ON THE LIABILITY OF INTERNET INTERMEDIARIES (2007), *available at* http://ec.europa.eu/internal_market/e-commerce/docs/study/liability/final_report_en.pdf.

164. 12 U.S.C. § 512 (c) (2006).

165. *See generally* Daniel Solove, *Speech, Privacy and Reputation on the Internet*, *in* THE OFFENSIVE INTERNET: PRIVACY, SPEECH, AND REPUTATION 25 (Saul Levmore & Martha C.

> [w]henever bloggers or website operators know that a comment posted by another is tortious, the law should create an incentive for them to remove it. If a person promptly removes a tortious comment after being notified, then that person would be immune. If the person fails to remove the comment, only then would the person be subjected to potential liability.[166]

The provision could be modeled after the DMCA provision regarding notice and takedown of allegedly infringing copyrighted material. Some critics argue that the DMCA takedown provision has been abused by copyright owners who use it to remove lawfully posted material and that such a provision under section 230 would be similarly abused.[167] Daniel Solove tackles such criticisms, noting that while the DMCA is "fraught with problems, as zealous copyright owners are making overbroad takedown requests for material that is fair use,"[168] a similar provision under section 230 is unlikely to be abused in that way:

> Would notice and takedown for defamatory or privacy-invasive speech run into similar problems? I do not believe it would for several reasons. First, abusing the notice-and-takedown system should be penalized. Those who wrongly issue takedown threats for material that is not defamatory or invasive of privacy should be punished for making unjustified claims. Second, the entities enforcing copyright law are often very wealthy, powerful and aggressive. . . . In contract, most privacy or defamation plaintiffs are ordinary individuals, without the ability to hire armies of lawyers or to pursue cases relentlessly to the four corners of the globe. Most individuals who request information be taken down to protect their personal reputations lack the litigating power of the music or movie industry, and the stakes are much lower.[169]

Solove acknowledges that there is the possibility of excessive takedown and predatory lawsuits that aim to extort money.[170] In response to predatory lawsuits, he proposes mandatory mediation and limits on damages.[171] Solove's response to the risk of excessive takedown, however, is less definitive. He states that "[l]essening §230 immunity is unlikely to increase the existing risk of excessive takedown in a dramatic fashion."[172] But, Solove acknowledges that there are unanswered empirical questions regarding the impact of a

---

Nussbaum eds., 2010) (recommending that section 230 be modified to have a notice-and-takedown system rather than complete immunity); Bradley A. Areheart, *Regulating Cyberbullies Through Notice-Based Liability,* 117 YALE L.J. POCKET PART 41 (2007), *available at* http://thepocketpart.org/2007/09/08areheart.html (proposing a notice-and-take-down scheme similar to that available under the Digital Millennium Copyright Act); Rustad & Koenig, *supra* note 19, at 388 (arguing "that Congress should amend § 230 to reimpose a regime modeled on the common law's 'distributor with knowledge' principle.").

166. Solove, *supra* note 165, at 25.

167. *Id.* at 25–26.

168. *Id.* at 25.

169. *Id.* at 26 (citation omitted).

170. *Id.*

171. *Id.*

172. *Id.*

takedown regime upon legitimate speech and that the "only way to find out for certain is to experiment."[173]

Michael Rustad and Thomas Koenig propose a more concrete notice and takedown regime that addresses the potential problem of frivolous claims. Their proposal would give content creators the right to a federal court hearing to reverse unjustified takedown notices, and would impose penalties upon those making bad faith takedown demands.[174]

Some free speech advocates may find notice and takedown or notice-takedown-put back proposals unsatisfying, especially given the lack of public forums on the Internet and the cultural primacy placed upon freedom of speech in American society. Given the large amount of content on some websites, some argue that any notice and takedown regime places too great a burden on intermediaries to respond.

Notwithstanding these valid concerns, blanket immunity places too great a burden upon victims of online harassment. In an attempt to recalibrate the speech-privacy balance, this article proposes a notice-takedown scheme with a twist—a response-and-identification safe harbor. Upon receiving a takedown notice, the website operator may notify the poster and the poster may elect to stand by the posting by identifying herself. The posting would then become an "identified" posting and the website operator would be immune from civil liability.

The benefit of this safe harbor is that it shifts the burden of assessing content upon the poster. It forces the content creator—and not the intermediary—to make the sometimes difficult determination whether content is lawful. There is no incentive for the intermediary to remove content merely to avoid the possibility of a lawsuit. Rather, it is the content creator who must make the determination whether continued publication is worth the risk of being sued. Thus the risk of unlawful speech remains where it should be—with the speaker.

C. Nonprofit Companies with No Site Advertising

In some cases, a website may hold itself out to be a quasi-public forum, claiming that it serves a valuable social function by providing a virtual space to debate issues of public concern. The motivations of companies, however, may not be entirely pure. The argument about wishing to serve as a public forum sounds disingenuous where the site discussions primarily involve private figures and where the site profits from page views[175] or where the website

---

173. *Id.* at 26–27.

174. Rustad & Koenig, *supra* note 19, at 401.

175. On a related issue about the dichotomous nature of intermediaries, Rob Frieden pointedly observes that ISPs "toggle between claiming First Amendment-protected speaker rights and invoking 'safe harbor' exemptions from liability for the content they carry. . . . ISPs seemingly can turn on and off their speaker status to qualify for two different types of limits on government regulation of the content they deliver." Frieden, *supra* note 73, at 1281–82.

charges a fee to provide services to "arbitrate" disputed postings.[176] A company may claim to serve a public forum function *and* make money doing so, but in that case, it should be willing to accept ordinary business risks, including the risks of proprietorship liability. This third safe harbor would protect those intermediaries that are organized as nonprofits so long as they do not accept paid advertisements on their sites. This safe harbor distinguishes between those sites that serve public forum functions, and those which merely employ such rhetoric while running for-profit businesses.

D. Proposed Legislative Amendment

As previously discussed, section 230 of the CDA has been misinterpreted by courts to grant broad immunity to intermediaries. *There is nothing in the statutory language that grants immunity to intermediaries.* Furthermore, the only exculpatory language in the legislation is with regard to good faith efforts to remove or restrict access to objectionable material. Section 230(c)(1) merely defines the status of intermediaries in the negative; it does not explain what a publisher or speaker is, or in what context it would be appropriate to make such distinctions. The uncertain purpose of section 230(c)(1) is largely responsible for the judicial missteps with section 230 cases. Courts seem to have conflated the exculpatory language regarding good faith removal and restriction efforts in section 230(c)(2) with the language about not treating intermediaries as publishers or speakers in section 230(c)(1), to perversely grant broad immunity to websites *because* they are publishers of content. Given the judicial madness created by subsection (1), this article proposes that it be deleted and replaced with provisions that provide for targeted instances of immunity. To reflect these proposed safe harbors, and to clarify the imposition of civil liability, the language of section 230 of the Communications Decency Act should be amended as follows:

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

176. *Ripoff Report*, for example, provides a "V.I.P. Arbitration process" whereby a complaining party may seek to have a false statement redacted. *About Us: Want to Sue Ripoff Report?*, *supra* note 158. The program is not free, however, as the site notes "there is a cost for participating in the program which covers the arbitrator's fees and our administrative costs, but the program is not expensive compared with other alternatives." *Id.*

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

(C) Nothing in this section shall be construed to limit the civil or criminal liability of an interactive computer service provider or user except that:

i. no interactive computer service provider shall be liable for content provided by another information content provider if –

1. upon notice of the content by a complaining party, the interactive computer service provider acts expeditiously to remove, or disable access to, the content or, alternatively, identifies the information content provider with information sufficient to permit the complaining party to contact the information content provider (such as an address, telephone number and an electronic mail address) and provided further that the website operator expeditiously removes content if so requested by the information content provider;

2. all content posted on a website by information content providers are accompanied with a first and last name identifying the information content providers, and provided further that upon request by a complaining party, the website operator identifies the information content provider with information sufficient to permit the complaining party to contact the information content provider (such as an address, telephone number and an electronic mail address) and provided further that: (i) the website operator expeditiously removes the content upon request of the information content provider; and (ii) the website operator expeditiously removes the content if the name or contact information of the information content provider is false or unverifiable; or

3. the interactive computer service provider is a non-profit entity which does not earn any revenue or receive any monies from advertising on the website where the content that is the subject of a complaint is posted.

. . . .

(e) Effect on other laws

(3) State law

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

(f) Definitions

. . . .

(5) website operator

The term "website operator" means any person or entity, including any interactive computer service, that manages and has the ability to control the content on a website.

(6) website

The term "website" means a location on the Internet indicated by a Uniform Resource Locator or "URL."

IV. ANTICIPATED OBJECTIONS

Opponents to these proposals will likely respond in one of two ways. The first category of argument has to do with Internet growth and business innovation. The second category involves free speech. Both of these objectives are reflected in the policy goals of the CDA. In addition, this Part briefly addresses arguments that the aforementioned proposals do not go far enough to address online harms.

A. Business Arguments in Favor of Section 230

One argument in favor of section 230 immunity is that it promotes technological innovation and the growth of online businesses.[177] According to this view, the specter of tort liability for intermediaries would have a chilling effect on Internet businesses and innovation.[178] This article expresses skepticism that the threat of liability is likely to significantly hinder the growth of the Internet and the author is unaware of any empirical studies to support this often repeated claim. It is still much less costly to start a business online than it is to open a store or publish a book or magazine. The low costs of opening an online business (compared to the costs of opening a business that requires occupying physical property) and the increasing fluidity between online and offline transactions ensures that companies will continue to conjure up innovative online businesses. As the Ninth Circuit Court of Appeals remarked in a footnote in the *Roommates* case, "[c]ompliance with laws of general applicability seems like an entirely justified burden for all businesses, whether they operate online or through quaint brick-and-mortar facilities."[179] It further remarked that the vast reach of the Internet is "exactly why we must be careful not to exceed the scope of the immunity provided by Congress and thus give online businesses an unfair advantage over their real-world counterparts, which must comply with laws of general applicability."[180] In a world where

---

177. *See, e.g.*, Eric Goldman, *How 47 USC 230 Improves Marketplace Efficiency,* TECHNOLOGY & MARKETING LAW BLOG (Mar. 15, 2011), http://blog.ericgoldman.org/archives/2011/03/how_47_usc_230.htm; Cecilia Ziniti, *The Optimal Liability System for Online Service Providers: How Zeran v. America Online Got it Right and Web 2.0 Proves It,* 23 BERKELEY TECH. L.J. 583, 616 (2008) (noting that while it is unclear to what extent whether section 230 immunity assisted the development of Web 2.0, it poses less hurdles to it than alternatives).

178. Alex Kozinski and Josh Goldfoot recently wrote:

> [T]he "argument that a legal holding will bring the [I]nternet to a standstill makes most judges listen closely. . . . No one in a black robe wants to be responsible for anything like that . . . Closely related is the argument that, even if you don't bring down the existing structure, the threat of liability will stifle innovation, so that the progress we have seen in recent years—and the gains in productivity and personal satisfaction—will stop because the legal structure has made innovation too risky or expensive.

Alex Kozinski & Josh Goldfoot, *A Declaration of the Dependence of Cyberspace,* 32 COLUM. J.L. & ARTS 365, 370 (2009). One of the authors, Alex Kozinski, is the chief judge of the United States Court of Appeals for the Ninth Circuit. The authors conclude that the innovation argument is "partly right, but mostly wrong." *Id.*

179. Fair Hous. Council of San Fernando Valley v. Roommates.com, L.L.C., 521 F.3d 1157, 1169 n.24 (9th Cir. 2008).

180. *Id.* at 1164–65 n.15.

print magazine and newspaper subscriber bases and advertising revenues are being siphoned away by online publishers, an immunity for online publishers that is unavailable for offline ones is simply discriminatory and unfair.

There is a tendency to refer to Internet companies as a singular type when, as this article has explained, there are a wide variety of business models, practices and policies. All businesses are not good for society, and all Internet companies are not innovative. Websites that encourage defamatory content or content that invades the privacy of private citizens do so in contravention of society's values. Of course, there may be websites that would be threatened by reducing the scope of section 230 immunity. Many consumer review websites, for example, might disappear or be forced to change their submissions policies.[181]

The disappearance of these websites would not be tragic or notable. Companies have always had to assess risks, including the risks of litigation, with the potential upside of engaging in business. The extremely low barriers to entry have changed the typical Darwinian process of survival represented by a free market system. The result is more and more unreliable consumer review websites and an increasing scarcity of quality reporting. Readers of a traditional publication, such as the *New York Times*, are often familiar with a particular reviewer's tastes and preferences. They trust that reviewer, even if they do not agree with that reviewer's opinion. They know, in other words, where that reviewer is coming from. It is a different story with online review sites. The consumer searching for a recommendation is barraged with information, forced to sift through the offerings of many review websites and to assess the reliability of the often wildly diverging reviews without knowing where the reviewers are coming from or whether their tastes and preferences align with the consumer. The reviews may be disingenuous or dishonest.[182] Some of the negative reviews may be the result of vengeful and petty customers or competitors, and some of the positive reviews may be from company employees. The reduction of online consumer review sites may prove beneficial for consumers who already suffer from information overload. Companies may institute more rigorous review policies or may establish themselves in ways to qualify for a safe harbor provision. Far from sounding a death knell for consumer review sites, imposition of proprietorship liability may result in a decrease in their quantity but an increase in their quality, reliability, and usefulness.[183]

---

181. Eric Goldman credits section 230 with enabling the proliferation of consumer review publications. Goldman, *supra* note 177. He notes that "47 USC 230's immunity enables consumer review websites," which help "consumers make better marketplace decisions." *Id.*

182. Eric Felten, *Lawsuits Fly Over Mean Online Reviews*, WALL ST. J., Apr. 23, 2010, at W11 (remarking that "even the most cursory perusal of online comments that rate products and services also discovers plenty of manufactured praise and malicious trash-talk"). Not surprisingly, many people "question the honesty of online critiques." *Id.*

183. David Segal, the consumer advocate columnist writing *The Haggler* for the *New York Times*, recently wrote about the problem of fake reviews on consumer review websites such as Yelp where businesses can pay to have someone post a favorable review about their company. David Segal, *A Rave, a Pan, or Just a Fake?* N.Y. TIMES, May 22, 2011, at BU7. In another col-

Eric Goldman has referred to section 230 as reflecting an "Internet exceptionalist" view because it "treats online providers more favorably than offline publishers—even when they publish identical content."[184] Internet exceptionalists believe that cyberspace is different from real space and that different rules and principles should apply.[185] The Internet exceptionalist view exhibits an unfortunate tendency to refer to technology and innovation as characteristics specific to Internet-based businesses.[186] Yet, technology does not happen only or even primarily online. There are many businesses that are working on products and services to improve human lives.[187] Pharmaceutical companies are working on drugs to prevent cancer or alleviate pain. Clean technology companies are searching for alternative fuel sources and researching ways to reduce carbon emissions. Yet, these companies do not benefit from broad immunity for their actions. Online consumer review sites such as Yelp should not receive immunity from tort liability when more socially beneficial companies (for example, a biotech start-up working on a treatment for Alzheimer's disease) do not. If a few would-be online entrepreneurs decide to pursue alternative career paths because of the fear of tort liability, our society will survive. In fact, it may even flourish. For-profit businesses have never been, and should never be, risk-free. As Chief Judge of the United States Courts of Appeals for the Ninth Circuit, Alex Kozinski, and his coauthor, Josh Goldfoot, write:

> [P]romoting innovation alone cannot be a sufficient justification for exempting innovators form the law. An unfortunate result of our complex legal system is that almost everyone is confused about what the law means, and everyone engaged in a business of any complexity at some point has to consult a lawyer. If the need to obey the law stifles innovation, that stifling is just another cost of having a society ruled by law.[188]

Companies have always engaged in a calculated analysis of the costs and benefits of engaging in a particular type of business. Section 230 immunity

---

umn, Segal noted that one review site, *Transport Reviews*, generates revenues from transport companies, which can buy advertisement and a higher profile on the site. The website also permits companies to post the last response to any negative review. David Segal, *Sure, Post A Review. But the Last Word Won't Be Yours*, N.Y. TIMES, Nov. 27, 2011, at BU8.

184. Eric Goldman, *The Third Wave of Internet Exceptionalism*, TECHNOLOGY & MARKETING LAW BLOG (Mar. 11, 2009), http://blog.ericgoldman.org/archives/2009/03/the_third_wave.htm.

185. *See, e.g.*, David G. Post, *Against "Against Cyberanarchy"*, 17 BERKELEY TECH. L.J. 1365, 1366 (2002) (noting that "[c]ommunication in cyberspace is not 'functionally identical' to communication in realspace—at least, not in ways relevant to the application of the choice-of-law and jurisdictional principles under discussion").

186. *See* discussion *infra* Part IV.B.

187. Kenneth Frazier, the president and CEO of Merck & Co. recently wrote that "the life sciences are largely absent from most discussions about encouraging innovation, while the extensive research and development that stands behind each new vaccine of medicine is invisible to all but a few. Most Americans have no clue about the extraordinary scientific innovation and huge R&D investment embodied in the small pill or capsule their doctors prescribe." Kenneth C. Frazier, *Will Washington Find the Cure for Cancer?*, WALL ST. J., July 13, 2011, at A17.

188. Kozinski & Goldfoot, *supra* note 178, at 371.

gives online intermediaries an unfair advantage over their offline counterparts. It also skews society's sense of values and Wall Street's valuation sense.[189] Facebook may soon have a billion users but it is really more valuable to society than a company that is researching a cure for cancer? Given the potential for rich financial rewards, shouldn't online companies be willing to bear some of the risks of their business models?

The threat of liability may actually spur some types of innovation by creating a market need.[190] Some companies may develop technologies that assist other companies in minimizing the risk of civil liability. For example, Facebook recently adopted Microsoft's PhotoDNA technology to detect child pornography on its site.[191] Critics have argued that social networking sites should do more to prevent predators on their sites from exploiting children. Microsoft created the product to address a social problem and Facebook adopted the technology in response to market pressure.[192] Similarly, proprietorship liability may create a market need that may, in turn, spur innovation as entrepreneurs create products that enable other companies to reduce the risk of liability.

On the other hand, broad immunity may promote technology that is socially harmful. It may encourage the development of even sneakier ways to take unauthorized photographs and recordings or it may lower their cost and make the existing technology accessible to more consumers. There may be less consideration given to (and thus less effort to prevent) the negative consequences of technological innovations.[193] As Kozinski and Goldfoot note:

> There is an even more fundamental reason why it would be unwise to exempt the innovators who create the technology that will shape the course of our lives: granting them that exemption will yield a generation of technology that will shape the course of our lives: granting them that exemption will yield a generation of technology that facilitates the behavior that our society has decided to prohibit. If the [I]nternet is still being developed, then we should do

189. Facebook's recent public offering valued that company at $104 billion. *See* Shayndi Raice et al., *Facebook Prices IPO at Record Value,* WALL ST. J. (May 17, 2012), http://online.wsj.com/article/SB10001424052702303448404577409923406193162.html.

190. A similar point is that imposing tort liability may provide an incentive for intermediaries to implement consumer protective measures. Rustad and Koenig note that an interactive computer service provider is "in the best position to develop comprehensive authentication systems to reduce anonymous crimes and torts in cyberspace. . . . However, absent a change in ISP law, [they have] no responsibility to lend a hand to consumers who are victimized by online frauds even if the ISP can readily uncover the wrongdoer's contact information." Rustad & Koenig, *supra* note 19, at 391.

191. Ernie Allen, *Facebook to Use Microsoft's PhotoDNA Technology to Combat Child Exploitation*, MICROSOFT (May 19, 2011, 8:00 AM), http://blogs.technet.com/b/microsoft_on_the_issues/archive/2011/05/19/facebook-to-use-microsoft-s-photodna-technology-to-combat-child-exploitation.aspx.

192. *Id.*

193. Patricia Leigh Brown, *In Oakland, Redefining Sex Trade Workers as Abuse Victims*, N.Y. TIMES, May 24, 2011, at A13. Brown describes the problem of "American-born minors lured into the sex trade" as one that has "exploded with the Internet." *Id.*

> what we can to guide its development in a direction that promotes compliance with the law.[194]

Facial recognition technologies, for example, have raised privacy concerns because they are being introduced into consumer goods and on social networking sites.[195] The possibilities of combining broad website immunity, anonymous postings and the two regrettable behaviors are chilling and may threaten what privacy that we do have—privacy that is already greatly diminished by technological advancements. Website operators may be more thoughtful about how and whether to employ such technologies if they lose their broad immunity.

The burdens of proprietorship liability should not be exaggerated. The standard is not one of strict liability nor a heightened one, but one of ordinary reasonableness. It merely permits an inquiry into the reasonableness of a website proprietor's conduct. By that standard, most of our cherished Internet companies would still be in business as they already strive to conform to socially acceptable business practices and are typically responsive to customer complaints. Google will continue to thrive; TheDirty.com will not.

Significantly, online entities have ways to reduce the risks of doing business and have a way to alleviate the burdens from lawsuits. They can require their users to indemnify the site from third-party lawsuits arising out of content posted by the user. They can require visitors (and not just posters) to click to agree to certain contractual terms, such as mandatory arbitration, forum selection, and attorneys' fees before accessing the site.[196] The website operator may also avail itself of one of the proposed safe harbors by permitting content only by identified posters, responding to takedown requests or organizing itself as a nonprofit and refusing to accept paid advertisements.

One might argue that revising section 230 immunity is unnecessary because socially harmful businesses, such as gossip sites, will eventually be driven out by the invisible hand of the marketplace. This reliance on market forces, however, ignores the economics of the Internet and the way that section 230 forces any such hand. Web-based businesses generally have much lower start-up and operating costs than their counterparts in the offline world. For example, the founder of 4chan, a website created in 2003, which attracts mostly advertisers in the adult entertainment industry, said that his site generates advertising revenue in the "low five figures."[197] Yet, he started the site when he was only fifteen years old and has been able to keep it running for nearly a decade. A publisher of books and magazines has much greater costs

---

194. Kozinski & Goldfoot, *supra* note 178, at 371.

195. Emily Steel, *A Face Launches 1,000 Apps,* WALL ST. J., Aug. 5, 2011, at B5 (noting the concern that privacy advocates have over how facial recognition technology is used by companies that employ them).

196. *See* Kim, *supra* note 17, at 1014–19 (proposing contractual and design strategies to deter cyber harassment).

197. Jenna Wortham, *Founder of a Provocative Web Site Forms a New Outlet,* N.Y. TIMES, Mar. 14, 2011, at B1. The *New York Times* reported that 4chan is "one of the largest forums on the Internet" and considered "one of the darkest corners of the Web." *Id.*

than an online publisher of content. Yet, book and magazine publishers are not immune from liability the way online publishers are under section 230. Section 230 puts an enormous thumb on the scale that typically weighs free market forces, tilting the balance in favor of online companies.

The invisible hand argument also ignores the multiplicity of ways that websites can generate monetary gain for their operators. Even if the websites themselves do not generate much revenue, the proprietors of these websites reap the benefits of high visibility and can receive book contracts, speaking invitations and offers to invest in future online ventures.[198]

More importantly, the invisible hand argument ignores the realities of online harm. Even if the invisible hand eventually drives some sites out of business, the content that was posted while they existed may remain searchable and accessible online. The "invisible hand" argument too easily dismisses the very real harm to the victims of these businesses. For victims of online harassment, any website that enabled the ruination of their lives was in business too long.[199]

B. Section 230 and Free Speech

A common protest raised whenever the issue of amending section 230 arises is that anything other than broad immunity would chill speech.[200] Yet, First Amendment doctrine recognizes limits on speech.[201] The salient issue is not *whether* limits to online speech should exist, but *what* those limits should be. As Cass Sunstein notes:

> New technologies have greatly expanded the opportunity to communicate obscene, libelous, violent, or harassing messages . . . . Invasions of privacy are

198. The founder of 4chan, for example, launched a career as public speaker, an investment fund adviser, and founder of a new, venture-backed website. *Id.*

199. *See* Lipton, *We the Paparazzi*, *supra* note 10, at 983 (noting that privacy invading digital recordings may have "serious long-term consequences for many people").

200. Danielle Keats Citron observes that limiting abusive online communications may protect First Amendment values such as democratic governance. Citron, *supra* note 3, at 101–03. Cass Sunstein notes that the goals of the First Amendment are "closely connected with the founding commitment to a particular kind of polity: a deliberative democracy among informed citizens who are political equals." Cass Sunstein, *The First Amendment in Cyberspace*, 104 YALE L.J. 1757, 1800 (1995). He cautions that "[f]ree speech doctrine, with its proliferating tests, distinctions, and subparts, should not lose touch" with the purposes of the First Amendment and that "instead of allowing new technologies to use democratic processes for their own purposes, constitutional law should be concerned with harnessing those technologies for democratic ends—including the founding aspirations to public deliberation, citizenship, political equality, and even a certain kind of virtue." *Id.*

201. *See* Citron, *supra* note 3, at 106–10 (explaining how First Amendment doctrine does not protect threats, defamatory statements and emotional distress claims). *See, e.g., In re Verizon Internet Services, Inc.*, 257 F. Supp. 2d 244, 246 (D.D.C. 2003). The Recording Industry Association of America sought the identity of an anonymous user of Verizon's service who is alleged to have infringed copyrights by offering hundreds of songs for downloading. The court stated, "But when the Supreme Court has held that the First Amendment protects anonymity, it has typically done so in cases involving core First Amendment expression. . . . The DMCA . . . does not directly impact core political speech, and thus may not warrant the type of 'exacting scrutiny' reserved for that context." *Id.* at 259–60.

> far more likely. The Internet poses special problems on these counts. As a general rule, any restrictions should be treated like those governing ordinary speech, with ordinary mail providing the best analogy. If restrictions are narrowly tailored, and supported by a sufficiently strong record, they should be upheld.[202]

But rather than recognizing the unique character of harms caused by online speech, the broad immunity of section 230 as (erroneously) applied by many courts ignores them, and then loosens offline speech restrictions. The First Amendment doctrine that has been crafted by the judiciary over the years to carefully balance free speech with societal harms has been jettisoned by section 230. Offline publishers have never been granted blanket immunity from liability for the works they publish. Even online, intermediaries are liable for copyright infringement where they fail to remove claimed copyrighted works after notice.[203] The argument in favor of website proprietorship liability is not one that favors a new law—rather, it favors a return to the law, and the standard of reasonableness, that governs the rest of our society.[204] It rejects the Internet exceptionalism that favors different rules and laws, or no law, for online conduct.[205] Print publishers and distributors are, to varying degrees, subject to liability for the content they publish and distribute. No offline publisher has broad immunity akin to that enjoyed by its online counterpart. Not only do web publishers enjoy the lower costs of publication and distribution, they also are freed from many of the oversight and control responsibilities required of nondigital publishers.[206] The vetting of content routinely undertaken by nondigital publishers, which results in more accurate, better written

---

202. Sunstein, *supra* note 200, at 1799.

203. *See* Digital Millennium Copyright Act, (codified as amended at 17 U.S.C. §§512, 1201–05, 1301–22 and 24 U.S.C. §4001) (2006) (making it unlawful to access a work protected by an antipiracy measure but contains a notice and takedown provision for ISPs).

204. *See* Richard A. Epstein, *Privacy, Publication, and the First Amendment: The Dangers of First Amendment Exceptionalism*, 52 STAN. L. REV. 1003, 1004 (2000) (noting the danger of "endowing the new challenges in cyberspace with such novelty that it becomes too easy to forget that the underlying problems have been with us for a very long time.") *Cf.* Lyrissa Lidsky, *Hit Lists: Cyber Incitement, Cyber Threats*, PRAWFSBLAWG (Apr. 8. 2011), http://prawfsblawg.blogs.com/prawfsblawg/2011/04/hit-lists-is-cyber-incitement-different.html (wondering whether the Internet is a game changer for First Amendment doctrine).

205. Epstein, *supra* note 204, at 1006. Epstein also notes the problems created by what he calls "'First Amendment exceptionalism,' that is the belief that the First Amendment weights the scales above and beyond what a sensible theory of freedom of speech, understood as part of a general theory of freedom, would require." *Id.*

206. As Richard Epstein notes:

> One recent question of some import concerns the liability of Internet operators for defamatory messages posted on their systems by others. The Communications Decency Act provides these web page operators with absolute immunity. The obvious points here are, first, that the plaintiff's preferred defamation action should be directed against the party who posted the message, assuming that she can find him; next, that it becomes virtually impossible to ask the proprietor of the network to maintain a constant surveillance of the content posted on various sites by the wide range of subscribers, some of whom are certain to hold extreme, malevolent, or outlandish views. But that said, how different is the problem here from an attempt to hold a newspaper responsible for the content of personal advertisements, or a lending library responsible for the contents of the books it sends into circulation or a broadcast station for the defamation of one of its guests?

Id. at 1005 (citation omitted).

content, is often absent from the sites of publishers that encourage the two regrettable behaviors. A reasonableness standard conforms to societal expectations of businesses while permitting adjustments to the way the law is applied where the online experience really is different from the offline one.

This article's proposals promote the values of free expression. Some free speech advocates may be concerned that two of the proposed safe harbors reduce the number of forums for anonymous speech. This is only an illusory concern as the reality is that truly anonymous online speech does not really exist anymore even if unveiling a poster may be difficult. True anonymity has already been eradicated by the greed of online intermediaries who are intent on making money through increasingly more privacy invasive technology. This technology can be used against posters, to strip them of their anonymity, under court order. In a sense then, this article's proposed Takedown Upon Notice-Right of Reply Poster Identification safe harbor provides a greater benefit to posters than the section 230 regime that currently exists. It gives posters the chance to reconsider and have removed a potentially defamatory post, one which may have been made in a hot-tempered emotional state. The poster may ultimately decide to stand by the post but then does so with the awareness that a lawsuit may ensue. The current regime of absolute immunity provides posters with a false sense of security, with many unaware that their veil of anonymity may be shredded in the event of litigation. It also gives them control over whether the post should continue to be published, unlike the current 230 regime that gives intermediaries sole control over content with no liability for their actions.

Often, the free speech argument is framed in terms of hard core libertarianism yet conveniently forgets that immunity was granted by government intervention. Rather than proposing new legislation or regulation, this article seeks to remedy the negative effects of existing legislation. Scaling back the scope of the CDA is actually a move *against* regulation because it is the existence of this regulation that is a major contributing problem to socially harmful behavior online. Whereas offline publishers and distributors bear some responsibility for the works they publish, online publishers have broad immunity, which may encourage them to act in a socially irresponsible manner. Without the broad blanket immunity that section 230 provides, many of the most socially harmful websites would not survive, or they would have to redesign their websites in a way that forces greater accountability from their users.

C. Same Side of the Fence Criticisms

Some "same side of the fence" arguments may be expected from those who agree that limits should be placed on section 230 immunity, but believe that my proposals do not go far enough or object to some or all of the proposed safe harbors. As previously noted, other scholars have made stronger proposals for a notice-and-take-down regime similar to that currently applicable under the DMCA.[207] Although such a regime is appealing for a variety of reasons,

207. *See* discussion *supra* Part III.B.

given the volume of postings on many websites and the difficulty of determining their lawfulness without a factual inquiry, a notice-and-take-down regime may leave some website operators unduly burdened. Accordingly, my proposals include safe harbors in addition to notice and takedown.

Admittedly, the proposals in this article will not prevent every type of online harm and should not be expected to do so. What they do is carefully balance the harms of online postings and the two regrettable behaviors against legitimate concerns raised by those who desire the retention of immunity. In this way, I hope to move the conversation regarding section 230 immunity "over the fence."

Some may argue that to accommodate Internet growth and innovation, we should relinquish norms, such as privacy, and succumb to the changes that the Internet brings. But this view is outdated, stuck in time circa the early 1990s. The Internet is no longer a niche medium used by a handful of tech savvy individuals and it should not be treated as such. What happens online does not stay online; it affects human lives and our society's norms of conduct and communication.[208] The Internet exceptionalist argument ignores that not all change is good or inevitable. The path forged by the most trollish Internet users and the free for all nature of discourse is not predetermined or immutable. Change is organic and can be shaped and molded. Law is one way to shape change, and section 230 has shaped online discourse in a very negative way.

Critics of my proposed legislative amendment may object that the prospect of liability means that website operators would be required to make difficult subjective decisions about the legality and legitimacy of certain postings. A website operator might overreact and remove even constitutionally permissible content in response to takedown requests, thereby chilling speech. Thus, the argument goes, to avoid sliding down the slippery slope toward censorship, law and policy makers should leave the Internet to regulate itself.

Contrary to what this argument suggests, a takedown request is not "Big Brother" censoring what a private citizen can reveal about oneself, but an individual's attempt to protect her privacy and right to expression against the intrusive or unwanted actions of another private citizen.[209]

208. Elias Aboujaoude has written about the ways that the online identifies of individuals has irrevocably damaged their offline selves. *See generally* ELIAS ABOUJADOUDE, VIRTUALLY YOU: THE DANGEROUS POWERS OF THE E-PERSONALITY (2011). He notes, for example, that "[t]he way we see and evaluate ourselves is changing as a function of new personality traits born and nurtured in the virtual world." *Id.* at 10.

209. *See* SOLOVE, *supra* note 18, at vii (noting that "[w]hen it comes to gossip and rumor on the Internet . . . the culprit is ourselves. We're invading each other's privacy and we're also invading our own privacy by exposures of information we later come to regret. Individual rights are implicated on both sides of the equation. Protecting privacy can come into tension with safeguarding free speech . . .").

Furthermore, there is another slippery slope that is too often left unmentioned. As uncivil discourse increases, it threatens to weaken the girding that enables speech and expression. An example can be found in the tragic example involving a Rutgers student, Tyler Clementi.[210] Clementi committed suicide after his roommate, Dharun Ravi surreptitiously recorded Clementi having a sexual encounter with another man in his dorm room and then posted it online. What Ravi exposed by his treacherous act was a very private side of Clementi that the latter did not wish to share with just anyone, much less with everyone. Not only had Ravi invaded Clementi's privacy, he wrested away his roommate's autonomy, taking from him control over a very fundamental and personal part of his life. As Sean Scott writes: "Allowing the right to privacy to preempt the First Amendment may not be as harmful to First Amendment values as has been suggested by some courts. Indeed, recognizing the privacy interest at stake allows us to retain our autonomy, our dignity and facilitates this experiment called democracy."[211]

The schism between online and offline realities is a mirage and Clementi was not the only one who was hurt by the two regrettable online behaviors. Friends of the perpetrators, expressed surprise that Ravi would have engaged in such conduct.[212] Ravi's act of recording Clementi in an intimate moment, without his permission, was a level of intrusion that was unthinkable and difficult to accomplish twenty years ago but which is now too easy to do. Ravi's offline demeanor reportedly did not correspond to his online one, which suggests an extreme disinhibition effect. Clementi, however, did not have the advantage of a different online "persona" to shield him from the public's glare. But neither did Ravi as his identity was soon revealed on the Internet and national newspapers, and he became the object of universal scorn. Ravi was ultimately convicted of invasion of privacy and bias intimidation, which is a hate crime.[213] He could have served up to ten years for his impulsive third-party post but served 20 days of a 30-day jail sentence.[214]

There are those who argue that rather than thinking of ways to punish and deter those like Ravi, we should "toughen up" those like Clementi. That presents the other, more dangerous, slippery slope. A failure to enforce minimal levels of civility opens up the very real danger of tumbling headlong into a society that sanctions bullying of its disempowered and its marginalized. Then, rather than tolerance and justice, treachery and abuse become societal norms. Danielle Keats Citron writes about the pernicious effects of trivializing the

---

210. *Times Topics: Tyler Clementi*, N.Y. TIMES, http://topics.nytimes.com/top/reference/timestopics/people/c/tyler_clementi/index.html (last updated Mar. 26, 2012).

211. Scott, *supra* note 9, at 744.

212. Amy Ellis Nutt, *Friends of Dharun Ravi and Molly Wei Support Pair Charged in Rutgers Sex Video Case*, RUTGERS STAR LEDGER (Oct. 3, 2010), http://www.nj.com/news/index.ssf/2010/10/friends_of_dharun_ravi_molly_w.html.

213. Kate Zernike, *Jury Finds Spying in Rutgers Dorm was a Hate Crime*, N.Y. TIMES, Mar. 17, 2012, at A1.

214. *Id.*; Kate Zernike, *Jail Term Ends After 20 Days for a Former Rutgers Student*, N.Y. TIMES, June 20, 2012, at A26.

harmful effects of cyber harassment and argues that "[b]ecause law is expressive, it constructs our understanding of harms that are not trivial."[215]

Without a minimal level of security, citizens no longer feel free to express themselves, in public spaces or in the privacy of their own homes. Their inability to control the distribution of their expressive activity—who gets to see them do what and with whom—diminishes their very right to expression. Expression then becomes the privilege of those who are socially untouchable, because of their wealth or power, or because their expression is considered within acceptable social norms. As Jacqueline Lipton writes in the context of digital video invasions of privacy,

> If we do not act now, privacy-destroying norms may become entrenched and it will be much more difficult to protect privacy in the future. . . .There is little downside to considering regulatory action to protect privacy. Regulation, imperfect as it may be, can be revised later, but today's video privacy incursions may have far-reaching and potentially devastating consequences.[216]

My proposals strive to recapture the autonomy that has been lost in recent years and aim to loosen the grip that the two regrettable online behaviors have on our culture.

215. Danielle Keats Citron, *Law's Expressive Value in Combating Cyber Gender Harassment,* 108 MICH. L. REV. 373, 377 (2009) (referring to the law's ability to recognize the distinct suffering of online gender harassment).

216. Lipton, *We the Paparazzi*, *supra* note 10, at 984.