WEB SITE PROPRIETORSHIP AND ONLINE HARASSMENT

Nancy S. Kim*

Although harassment and bullying have always existed, when such behavior is conducted online, the consequences can be uniquely devastating. The anonymity of harassers, the ease of widespread digital dissemination, and the inability to contain and/or eliminate online information can aggravate the nature of harassment on the Internet. Furthermore, section 230 of the Communications Decency Act provides Web site sponsors with immunity for content posted by others and no incentive to remove offending content.

Given the unique nature of online harassment, ex post punitive measures are inadequate to redress grievances. In this Article, I propose the imposition of proprietorship liability upon Web site sponsors who fail to adopt "reasonable measures" to prevent foreseeable harm, such as online harassment. I also introduce several proposals to deter online harassment that would qualify as reasonable measures. These proposals incorporate contractual and architectural restraints, limits on anonymity, and restrictions on posting certain types of digital images.

TABLE OF CONTENTS

 Associate Professor, California Western School of Law; Visiting Associate Professor, Rady School of Management, UC San Diego. This paper was presented at TPRC's 36th Research Conference on Communication, Information, and Internet Policy, held at George Mason University School of Law on September 26–28, 2008; the Conference of Asian Pacific American Law Faculty, held at Denver University School of Law on April 24–26, 2008; and a faculty workshop at the Loyola University of Chicago School of Law. I greatly benefited from the comments that were made by audience participants at these presentations. Ideas in this paper were also presented at the Law & Information Society Symposium: Intermediaries in the Information Society, Center on Law and Information Policy, Fordham Law School, held in New York, New York, on March 27, 2009; and the 22nd Annual Media and the Law Seminar, held in Kansas City, Missouri, on April 17, 2009. I would like to express my gratitude to Tom Barton, Ed Dauer, James Grimmelmann, and Cynthia Ho for their very helpful comments and suggestions on prior drafts of this paper. I would also like to express my appreciation to Janet Bowermaster, Larry Benner, Seth Burns, and Fred Yen for their helpful comments in discussions regarding this paper, to my research assistants, Melissa Henkel and Brian Suba, and to the conscientious editors at the Utah Law Review for their diligent efforts.

> *"Now, once you had communal fires and cooking and a higher calorie diet, the social world of our ancestors changed, too. Once individuals were drawn to a specific attractive location that had a fire, they spent a lot of time around it together. This was clearly a very different system from wandering around chimpanzee-style, sleeping wherever you wanted, always able to leave a group if there was any kind of social conflict. We had to be able to look each other in the eye. We couldn't react with impulsivity. Once you are sitting around the fire, you need to suppress reactive emotions that would otherwise lead to social chaos. Around that fire, we became tamer."*[1]

I. INTRODUCTION

Several female law students were the subject of malicious and obscene comments on AutoAdmit, a Web site catering to law school students.[2] The cruel nature of the posts, the hostile, unrepentant mob mentality of the anonymous posters, and the adamant refusal of the Web site operators to remove the offensive posts shocked the legal community and attracted media attention.[3] After repeated, unsuccessful requests to the Web site operator to remove the posts, two of the women sued, claiming that the posts caused them emotional distress and diminished their professional opportunities.[4] As part of the litigation, the identities of several of the posters were revealed.[5] One of the named defendants was later dropped from the case; he then sued the plaintiffs, alleging emotional distress and damage to *his* professional reputation.[6]

The AutoAdmit case illustrates the damage online harassment wreaks upon both the targets of the harassment and the harassers. Although the harm to targets of online smear campaigns is obvious, what is less evident is that the harassers also risk damage to their own reputations.[7] Online communication is often phrased as

---

[1] Claudia Dreifus, *A Conversation with Richard Wrangham*, N.Y. TIMES, Apr. 21, 2009, at D2 (noting that Richard Wrangham is a professor of biological anthropology at Harvard University and author of CATCHING FIRE: HOW COOKING MADE US HUMAN (2009)).

[2] *See* Ellen Nakashima, *Harsh Words Die Hard on the Web*, WASH. POST, Mar. 7, 2007, at A1; David Margolick, *Slimed Online*, PORTFOLIO.COM, Mar. 2009, http://www.portfolio.com/news-markets/national-news/portfolio/2009/02/11/TwoLawyers-Fight-Cyber-Bullying.

[3] Margolick, *supra* note 2.

[4] *Id.*

[5] *Id.*

[6] *Id.*

[7] One of the defendants in the AutoAdmit case claimed that the lawsuit has ruined his life. *Id.* Another defendant claims he has been unable to find a job as a result of the negative publicity surrounding the Web site and the litigation. *Id.*

expressive speech,[8] but the nature of online discourse is often shaped by the Web site itself. For example, the founder of AutoAdmit marketed the Web site as an alternative to message boards that filtered out inflammatory posts.[9] This Article adopts a new approach to the problem of online harassment or "cyberharassment"[10] by treating it primarily as a failure of business norms,[11] rather than as a matter of unfettered speech.

Framing online harassment as a private-sector problem resolves or reduces many of the free speech concerns raised by First Amendment advocates.[12] It empowers and encourages Web site sponsors to shape developing norms as part of good business practices. Setting expectations for user conduct empowers Web site sponsors to better control their Web site image (i.e., their "brand"). To require users to conform to the law and prevailing offline social norms reinforces positive community values, and reduces the likelihood of conflicts between and amongst users regarding expectations of conduct on a particular Web site.

---

[8] *See, e.g.*, Eugene Volokh, *Freedom of Speech and Information Privacy: The Troubling Implications of a Right to Stop People From Speaking About You*, 52 STAN. L. REV. 1049, 1051 (2000) ("While privacy protection secured by contract [turns out to be] constitutionally sound, broader information privacy rules are not easily defensible under existing free speech law.").

[9] Margolick, *supra* note 2.

[10] I use the term online harassment or "cyberharassment" to characterize the use of the Internet as a medium for disseminating harmful material about another individual. The definition is deliberately loose to accommodate different types of conduct.

[11] This Article argues that the social problem of online harassment is one that should be addressed by Web site sponsors. By "Web site sponsors," I refer to the companies and individuals who control or have the ability to control activity on the Web site. I am not referring to Internet service providers or other Web hosting companies (ISPs) that technically enable those businesses, unless those companies also sponsor or control the activity on the site (such as AOL, which provides Internet access but also sponsors its own message board). *See, e.g.*, People Connection Blog, http://www.peopleconnectionblog.com (last visited Sept. 1, 2009) (showing that AOL sponsors it own message board).

The volume of traffic that a single ISP transports is typically many times greater than that hosted by any single Web site sponsor. *See* Mark A. Lemley, *Rationalizing Internet Safe Harbors* 12 (Stanford Public Law Working Paper, Paper No. 979836, 2007), *available at* http://ssrn.com/abstract=979836 (noting that it is "simply impossible for a search engine—to say nothing of an ISP or bandwidth conduit—to cull through the literally billions of links and messages they process each day and identify all those messages and Web pages that may create liability under any law"). Accordingly, different standards should apply to ISPs and Web site sponsors, and I confine my discussion in this Article to Web site sponsors.

[12] This is not to suggest that government regulation is not an appropriate way to address the problem of cyberharassment, only that First Amendment issues are more relevant where the government is directly regulating conduct rather than where a private entity or industry creates and adopts its own standards. For a discussion of an Internet-based civil rights strategy, see generally Danielle Keats Citron, *Cyber Civil Rights*, 89 B.U. L. REV. 61 (2009) (arguing that cyberharassment harms ought to be understood and addressed as civil rights violations).

Currently, Web site sponsors exercise power over their Web sites in an inconsistent and self-serving manner. They exercise property-like control over certain aspects of the site, yet claim powerlessness when it comes to removing harassing content. More important, despite their ability to control content, Web site sponsors are immune from liability as publishers under section 230 of the Communications Decency Act of 1996 ("section 230").[13] Courts have generally interpreted this provision to grant broad immunity to Web site sponsors.[14] Section 230 thus places responsibility for content directly—and exclusively—upon those who create it, and absolutely relieves from liability the Web sites that profit (or hope to profit) from it.[15] Yet the immunity granted to them under section 230 as *publishers* should not mean that Web site sponsors should be free from all liability for harm arising from their businesses.

Courts should impose tort liability upon Web site sponsors for creating unreasonable business models and hold them accountable for irresponsible and harmful business practices. To hold Web site sponsors accountable for creating socially irresponsible Web sites applies a "reasonableness" standard to Internet businesses that currently applies to offline businesses.[16] What constitutes reasonable measures or reasonable business practices, however, should acknowledge and accommodate the differences between Internet and offline proprietorships, such as dramatically higher volume online.

Online harassment is often viewed through the prism of free speech. Attempts to curb the substance of what is being said online become mired in discussions of constitutional rights, and online "speech" is often analyzed in the same way as offline "speech."[17] Yet online communication is not the same as offline communication. Although harassment and bullying have always existed, when such behavior is conducted online, the consequences have different dimensions.

---

[13] Communications Decency Act of 1996, 47 U.S.C. § 230, 560–61 (2006).

[14] *See, e.g.*, Carafano v. Metrosplash.com, Inc., 339 F.3rd 1119, 1123 (9th Cir. 2003) (noting that doubts should be "resolved in favor of immunity"); Zeran v. America Online, Inc., 129 F.3d 327, 330 (4th Cir. 1997) (holding Communications Decency Act 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").

[15] *See* Rebecca Tushnet, *Power Without Responsibility: Intermediaries and the First Amendment*, 76 GEO. WASH. L. REV. 986, 1016 (2008) (noting that the Communications Decency Act uncouples ISP "property" ownership from responsibility). Tushnet proposes that Internet intermediaries' immunity should be tied to limits on their ability to control speech. *Id*. at 1015.

[16] *See* Fair Hous. Council of San Fernando Valley v. Roomates.com, LLC, 521 F.3d 1157, 1162 n.9 (9th Cir. 2008) (expressing concern with applying different rules for offline and online businesses). The Ninth Circuit stated: "[W]e 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." *Id.*

[17] *See* discussion *infra* Part VI.

The anonymity of harassers, section 230 immunity, the ease of widespread digital dissemination, and the inability to contain and eliminate online information change the nature of harassment when it is conducted on the Internet. To apply a First Amendment analysis without recognizing the ways in which online communication differs from offline communication leaves many of the harms created by online harassment unaddressed.

Although this Article proposes several strategies that Web site sponsors can implement to reduce the incidence of online harassment, it does so with the awareness that any solution must be flexible enough to accommodate technological evolution. The objective of this paper is not to provide static solutions to online harassment; rather, it is to propose a new way of looking at what is, in fact, a new and evolving problem. This Article explains how online harassment is not "just like" harassment offline, and argues that to apply existing free speech doctrine without recognizing those differences ignores the norm-shaping impact of Internet communication at this stage of technology adaptation and accommodation.[18] Although my proposals do not eliminate all forms of online harassment on all Web sites, they do encourage moving away from the impulsive "anything goes" culture that prevails on some Web sites,[19] to one that requires more reflection and accountability. My proposals thus seek to encourage First Amendment values rather than to chill expression, without falling prey to slippery-slope First Amendment absolutism. Thus, one objective of this Article is to reconcile the culture of the Internet with offline social norms of behavior.[20]

This Article attempts to avoid solutions that are overbroad by specifically delineating the problems at issue. Part II identifies and describes the various types of conduct that fall under the umbrella definition of "online harassment." It also provides a brief overview of current legal doctrines addressing the problem of online harassment.

Part III explains why existing legal remedies are inadequate to solve online harassment. Part IV proposes "reasonable measures" that Web site sponsors should take to reduce the incidence of online harassment on their sites. The proposals

---

[18] This is not to say that there are not legitimate free speech concerns in Internet communication. For a discussion of these concerns, see Dawn C. Nunziato, *The Death of the Public Forum in Cyberspace*, 20 BERKELEY TECH. L.J. 1115 *passim* (2005) (lamenting the lack of public forums in cyberspace); Stacey D. Schesser, *A New Domain for Public Speech: Opening Public Spaces Online*, 94 CAL. L. REV. 1791 *passim* (2006) (advocating the formation of state-sponsored Web sites that would constitute public forums for free speech).

[19] *See supra* note 9 and accompanying text.

[20] *See generally* Anne Wells Branscomb, *Anonymity, Autonomy, and Accountability: Challenges to the First Amendment in Cyberspaces*, 104 YALE L.J. 1639, 1647 (1995) (noting that "more and more often, confrontations are arising between the legal expectations of the real world and the developing 'netiquette' of the 'netizens' of cyberspaces" and acknowledging that "transferring legal norms from the real world may result in the application of rigid rules inappropriate to the cybercommunities and may jeopardize the full development of the information agora that the technology promises").

focus on deterring, rather than penalizing, online harassment. The proposals also consider the ways in which Web-based businesses are different from brick-and-mortar businesses. In particular, accounting for the high volume of traffic handled by some Web proprietors, the proposals do not impose prescreening obligations or require proprietors to make difficult subjective decisions regarding whether to remove user-supplied content.

Part V summarizes and further develops an argument that I first proposed elsewhere:[21] that tort law—in particular, a liability analogous to premises or business owner liability—may effectively be used to impose standards of conduct upon Web site sponsors.[22] I recommend adopting at least some of the proposals in Part IV as "reasonable measures" to prevent foreseeable online harassment. To require adoption of an anti-cyberharassment policy is consistent with section 230, as it holds the Web site sponsor accountable for its *own* actions or omissions, not for the content posted by third parties. Part VI addresses the constitutional issues raised by anti-cyberharassment policies.

This Article concludes that the problem of online harassment necessitates a change in the way we currently view the role of Web site sponsors. Web site sponsors are proprietors of businesses, not state-sponsored public forums. Some Web site sponsors have accepted the responsibilities that come with proprietorship by creating safeguards and designing Web sites that discourage unlawful activity.[23] By contrast, other Web site sponsors have exploited their section 230 immunity by intentionally adopting business models and designing their Web sites in ways that encourage online harassment.[24] Although they may be immune from liability as publishers of harmful content on their Web sites,[25] they should be held liable as proprietors for the creation of businesses likely to cause foreseeable harm to third parties.

II. WHAT IS CYBERHARASSMENT?

The term "online harassment" or "cyberharassment" is typically used to refer to Internet postings intended to embarrass, annoy, threaten, or bother another *individual* (as opposed to a social or political group or movement).[26] Some words capture specific types of cyberharassment. "Cyberstalking," for example, is the

---

[21] *See* Nancy S. Kim, *Imposing Tort Liability on Websites for Cyber-Harassment*, 118 YALE L.J. POCKET PART 115 *passim* (2008), *available at* http://yalelawjournal.org/images/pdfs/732.pdf.

[22] *Id.* at 118. Courts have rejected the premises-liability argument. I discuss the leading case rejecting premises liability and why the court's grounds for rejecting the theory was wrong in Part V.

[23] *See infra* note 164 and accompanying text.

[24] *See supra* note 9 and accompanying text.

[25] *See supra* notes 13–15 and accompanying text.

[26] Although harassment of a social or political group or organization, such as racial or religious minorities, constitutes cyberharassment, this Article focuses specifically on harassment targeted at individuals.

term most frequently used to describe the threatening, often anonymous stalking of an individual through chat rooms, e-mail, and other forms of instant communication.[27] Some forms of online harassment are not threatening as much as they are annoying or humiliating. Some commentators distinguish "cyberharassment" from "cyberbullying" by defining cyberharassment as directed at adults and cyberbullying as directed at students or children.[28] I use the term cyberharassment to include cyberbullying, but the range of conduct and communication makes the use of one term inadequate. The absence of precise terminology makes discussion of cyberharassment difficult. Consequently, proposals aimed at one type of conduct may be inappropriate (either under- or overinclusive) for other types of conduct.

The usefulness of the phrase cyberharassment as a broad, catch-all term makes it necessary to categorize the various types of conduct that fall under it. For example, cyberharassment covers both repeated and unwanted e-mail messages from known acquaintances, as well as threatening and aggressive blog postings from anonymous posters. It also covers distribution of video clips and digital images of a personal, embarrassing, or intimate nature. While all these examples share a commonality—the use of the Internet as the medium for distributing the communication—the maliciousness of the actions varies, as does the intended and likely effect upon the victim of the harassment. Accordingly, the solutions to prevent, deter, or punish such actions should also vary. Failure to delineate and categorize different types of conduct risks policy proposals and solutions that are overbroad or otherwise ill-suited for some problems, though appropriate for others.

To be useful, a characterization of forms of cyberharassment must recognize that words and images may be employed in a variety of ways and to different effects. Although online harassment can occur in closed arenas, such as through e-mail or closed group invitations, this Article is limited to online harassment that is conducted on publicly accessible Web sites, including those sites that require membership, so long as membership is nonselective and available to anyone who applies.[29] Certain online communication (e.g., e-mails, list-serve communications,

---

[27] *See, e.g.*, Harry A. Valetk, *Mastering the Dark Arts of Cyberspace: A Quest for Sound Internet Safety Policies*, 2004 STAN. TECH. L. REV. 2, 53–65 (defining cyberstalking).

[28] *See, e.g.*, Renee L. Servence, Comment, *Cyberbullying, Cyber-Harassment, and the Conflict Between Schools and the First Amendment*, 2003 WIS. L. REV. 1213, 1218–20 (distinguishing between cyberharassment and cyberbullying); Kara D. Williams, Comment, *Public Schools vs. MySpace & Facebook: The Newest Challenge to Student Speech Rights*, 76 U. CIN. L. REV. 707, 728 (2008) (distinguishing between cyberharassment and cyberbullying).

[29] For the sake of brevity, I will refer to Web sites that require membership, such as social networking sites, as "publicly accessible," where the contents of those sites are available to all members and membership is nonselective. In other words, if the content is available only to invited viewers, then that site, or portion of that site, is not publicly accessible. If the content is accessible if one registers with the site, and registration is automatically granted, then that site is publicly accessible for the purposes of this Article.

and invitation-only Web sites that require passwords and whose contents are not searchable) should be accorded greater protection than publicly disseminated speech because closed-communication speech is already restricted in its manner of distribution. Furthermore, for reasons discussed in Part III, publicly viewable and searchable information has the potential to cause greater harm than restricted Web sites.[30]

This Part provides a description of the various forms of online harassment by dividing harassing conduct into two general categories—verbal and visual/auditory—which will be used in the remainder of the Article.

A. Verbal Cyberharassment

Words convey meaning online, but not necessarily in the same way as in the physical world. Words may be used to communicate intent to harm another. They may also be used simply as a way to express oneself, but even nonmalicious communications may incidentally harm another.

1. Online Threats

- A software developer is attacked on various blogs, including her own, and threatened with rape, mutilation, and strangulation, including a statement that it would be a "pity if you turned up in the gutter where you belong, with a machete shoved in that self-righteous little cunt of yours."[31]

- A marketing consultant is threatened with bodily harm because of his blog posts.[32]

The expression of intent to inflict harm upon a person that causes the person to reasonably fear for his or her safety constitutes an "online threat" when such expression is communicated through the medium of the Internet. Cyberstalking is a pattern of repeated, credible online threats. Systematic and organized online threats may constitute cyberterrorism, as further explained below.

---

[30] Cyberharassment on closed Web sites also causes harm to its victims; however, to avoid being overbroad, this Article focuses on problems that are particular to publicly accessible Web sites. For example, "invitees" to password-protected sites are not members of the general public, and my analysis and application of tort law in Part V is consequently restricted to business owner liability to invitees of publicly accessible Web sites. Nevertheless, many of the issues raised in this Article could be applied to closed Web sites.

[31] *See* Citron, *supra* note 12, at 64–65; *see also* Kathy Sierra, *Creating Passionate Users*, http://headrush.typepad.com (Apr. 6, 2007) (discussing why she has removed the post that generated threats).

[32] Alex Pham, *Cyberbullies' Abuse, Threats Hurl Fear Into Blogosphere*, L.A. TIMES, March 31, 2007, at C1.

2. Online Insults

- The image of a boy with a rare congenital disease is posted on a Web site where users cruelly ridicule his appearance, calling his appearance "fucking hilarious," "frighteningly akin to the Joker from the Dark Knight movie," and a "grotesque sin."[33]

Insults are words that are used to offend, deride, or embarrass another. Online insults differ from online threats because the target or subject of the insult does not feel threatened. He or she may feel embarrassed or offended, but does not feel frightened or in danger as a result of the insult. An online insult would include opinions about an individual, or an occurrence involving that individual.

3. Online Gossip

- Women are encouraged to anonymously post information on a public Web site about their exes, such as whether they are promiscuous, have sexually transmitted diseases, and have illegitimate children.[34]

- An anonymous user posts on a popular social networking site that another family in the user's neighborhood has a son—identified by name—who "has been to jail" and dates "underaged girls."[35]

Gossip is the spreading of rumors or personal information about others. Gossip is distinguishable from insults in that it is presented as "factual." Gossip includes both rumors that are later substantiated as accurate, as well as falsehoods.

4. Online Confessions

- A blogger reveals explicit sexual information about her identifiable partners, including that one enjoyed being spanked, another was married, and that a third paid her for sex.[36]

---

[33] *See* Encyclopedia Dramatica, *Daniele Fiorezna*, http://www.encyclopediadramatica.com/Daniele_Fiorenza (last visited Sept. 1, 2009).

[34] *See* DontDateHimGirl.com, http://dontdatehimgirl.com (last visited Sept. 1, 2009); *see also* Lizette Alvarez, *(Name Here) is a Liar and a Cheat: Don'tDateHimGirl.com*, N.Y. TIMES, Feb. 16, 2006, at G1.

[35] *See Shhh! The Rise of Real People Internet Gossip Sites*, http://blog.nj.com/digital life/2008/06/heard_a_juicy_rumor_about.html (June 24, 2008, 6:25).

[36] *See* April Witt, *Blog Interrupted; When Jessica Cutler Put Her Dirty Secrets on the Web, She Lost Her Job, Signed a Book Deal, Posed for Playboy and Raised a Ton of Questions About Where America is Headed*, WASH. POST, Aug. 15, 2004, at W12.

- The wife of a Broadway mogul reveals on a popular video-sharing site that she discovered her husband's stash of porn and Viagra, and claimed that he was likely having an affair.[37]

Confessions are revelations of intimate details about oneself and one's relationships with others. Online confessions include personal blogs and information posted on social networking sites. In addition, online confessions may be captured in the form of a video clip.

5. Cyberdeception

- A thirteen-year-old girl commits suicide after communicating with a woman who was posing as a teenage boy through a fake MySpace account.[38]

- A man posing as a woman posts an ad on a popular message board seeking a "brutal dom muscular male." He then posts on his blog the names, pictures, e-mail addresses, and phone numbers of the men who respond.[39]

On the Internet, as the oft-quoted New Yorker cartoon states, nobody knows that you're a dog.[40] In some cases, the ability to disguise oneself and masquerade as someone else has led to tragic consequences.[41] The ease of hiding one's true identity and the use of communication tools to forge relationships make cyberdeception especially devious, particularly given that there is sometimes no crime for the resulting emotional wrongs.[42]

---

[37] *See The Advent of "YouTube Divorce" or Just Old-Fashioned Revenge?*, http://latimesblogs.latimes.com/webscout/2008/04/the-advent-of-y.html (Apr. 16, 2008, 12:14 PT).

[38] *See* Kim Zetter, *Cyberbullying Suicide Stokes the Internet Fury Machine*, WIRED.COM, Nov. 21, 2007, http://www.wired.com/politics/onlinerights/news/2007/11/vigilante_justice.

[39] *See* Mattathias Schwartz, *Malwebolence*, N.Y. TIMES MAG., Aug. 3, 2008, at 24, 26.

[40] *See* Peter Steiner, *On the Internet, Nobody Knows You're a Dog*, Cartoon, THE NEW YORKER, July 5, 1993, at 61.

[41] *See* Jennifer Steinhauer, *Verdict in MySpace Suicide Case*, N.Y. TIMES, Nov. 27, 2008, at 25 (discussing how a forty-one-year-old woman disguised as a teenage boy harassed a teenage girl who subsequently committed suicide).

[42] *Id.* (noting there was no existing crime under Missouri law for cyberdeception).

6. Cyberterrorism

- A female blogger and software developer suspends her blog and cancels public appearances after being attacked online, including having hackers reveal her home address and Social Security number.[43]

- A woman who had engaged in cyberdeception resulting in the suicide of a teenage girl finds herself the target of online mobs who reveal her e-mail address, satellite images of her home, and her phone numbers.[44] She becomes the subject of death threats, including having a brick thrown through her kitchen window.[45]

In some cases, harassers take action beyond communicative activity. Cyberterrorism is the use of intimidation in a systematic way to achieve a particular objective, other than pure communication. Cyberterrorists may hack into a victim's e-mail or online banking accounts, publicly reveal personal data such as Social Security numbers, and initiate online campaigns aimed at shutting down the victim's personal Web site or blog.[46]

B. The Use of Images in Online Harassment

- Pedophiles swap images of children online.[47]

- School children surreptitiously snap pictures of their classmates undressing during gym class and post the photographs to a public Web site.[48]

- A group of children forces a classmate to engage in humiliating acts while videotaping him. The video is then posted to a public Web site for other classmates to view.[49]

---

[43] *See* Citron, *supra* note 12, at 64–65; *see also* Jessica Valenti, *How the Web Became a Sexists' Paradise: Everyone Receives Abuse Online but the Sheer Hatred Thrown at Women Bloggers Has Left Some in Fear for Their Lives*, THE GUARDIAN, Apr. 6, 2007, at 16.

[44] *See* Schwartz *supra* note 39, at 26–27.

[45] *Id.*

[46] *See* Citron, *supra* note12, at 64–65; Valenti, *supra* note 43, at 16 (discussing how Kathy Serra, a blogger and software developer, was attacked on her own blog and on other Web sites when posters revealed her home address and Social Security number).

[47] *See* Kurt Eichenwald, *From Their Own Online World, Pedophiles Extend Their Reach*, N.Y. TIMES, Aug. 21, 2006, at A1.

[48] *See* INTERNATIONAL ONLINE CONFERENCE REPORT, NEW FORMS OF SCHOOL BULLYING AND VIOLENCE: CYBERBULLYING, HAPPY SLAPPING AND OTHER NEW TRENDS 9 (Apr. 24–May 19, 2006), *available at* http://www.bullying-in-school.info/uploads/media/Conference_3_-_full_Report.pdf.

- A woman claims that her ex-boyfriend has a sexually transmitted disease and posts his photograph and name on a publicly searchable social networking site.[50]

- A jilted boyfriend vengefully posts nude pictures of his ex-girlfriend online.[51]

Online harassment may involve the use of images, such as photographs or videos. Although the method by which such images are captured may vary, for purposes of this Article's analysis, all images—whether captured as a photograph, video, or document—are classified simply as images. Images may accompany an online confession. For example, an individual may post a video of herself talking about an impending divorce.[52] In such cases, the words spoken by the individual should be viewed as an online confession and the video image (of the individual or others) should be analyzed as distinct from her confession. An image often reveals more information, and it therefore has the potential to be more damaging than a written description. For example, a blogger's description of her lover's face or naked body is likely to be less revelatory (and invasive to the lover's privacy) than posting his picture. As discussed in Part VI, the posting of certain images should not be equated with speech protected by the First Amendment.

III. THE NEED FOR ALTERNATIVE APPROACHES TO CYBERHARASSMENT

Part III explains why existing remedies are inadequate to address the problem of online harassment. It then proposes reframing the problem of online harassment as a failure of business norms rather than as a constitutional right to expression.

A. An Overview of Existing Remedies

Laws currently address some, but not all, of the crimes that now fall under the umbrella definition of online harassment. This Part is not intended to be an exhaustive exposition of such remedies; nor is it a discussion of the various conceptions of privacy. Rather, it is intended to provide some necessary

---

[49] *Id.*

[50] *See* DontDateHimGirl.com, http://dontdatehimgirl.com (last visited Sept. 1, 2009).

[51] *See* Richard Morgan, *Revenge Porn*, http://men.style.com/details/blogs/details/porn_punishment/index.html (November 2008); Barnes v. Yahoo!, No. Civ. 05-926-AA, 2005 WL 3005602 (D. Or., Nov. 8, 2005) *rev'd on appeal* 2009 WL 1232367 (9th Cir., May 7, 2009) (plaintiff's ex-boyfriend posted nude pictures of plaintiff to Yahoo's online chat rooms).

[52] One high-profile divorce video garnered over three million views. *Trisha Walsh-Smith–The Video That Started it All!*, http://www.youtube.com/watch?v=hx_WKxqQF2o (last visited Sept. 1, 2009).

background to frame the proposals offered in Part IV.[53] Generally, the remedies currently available to victims (of some types) of online harassment can be grouped in three broad categories: (1) tort actions deriving from privacy, (2) nonprivacy tort claims such as defamation and intentional infliction of emotional distress, and (3) criminal or anti-stalking statutes.

1. Tort Actions Deriving from the Right to Privacy

The primary remedies for victims of online harassment derive from the right to privacy. Samuel Warren and Louis Brandeis first recognized privacy as a legal right in a groundbreaking article.[54] Warren and Brandeis described the "right of privacy" as a natural development of the common law:

> That the individual shall have full protection in person and in property is a principle as old as the common law; but it has been found necessary from time to time to define anew the exact nature and extent of such protection. Political, social, and economic changes entail the recognition of new rights, and the common law, in its eternal youth, grows to meet the demands of society.[55]

As many scholars have noted, however, although courts have recognized the existence of a "right to privacy," the parameters of such a right are vaguely defined.[56]

The recognition of a right to privacy[57] gave rise to several common law actions in tort, namely appropriation,[58] false light,[59] disclosure or wrongful

---

[53] For a helpful taxonomy that characterizes privacy by violations rather than existing causes of action, see Daniel J. Solove, *A Taxonomy of Privacy*, 154 U. PA. L. REV. 477, 481–83 (2006). Employing Solove's taxonomy may alleviate many of the problems arising from the public/private distinction.

[54] Samuel Warren & Louis Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 193 (1890). While the concept of privacy existed prior to publication of Warren and Brandeis's article, the article is widely acknowledged as being the first to establish the legal foundation for such a right. For further discussion on privacy as a legal right, see Solove, *supra* note 53, at 481–83, and Katherine Strandberg, *Privacy, Rationality, and Temptation: A Theory of Willpower Norms*, 57 RUTGERS L. REV. 1235, 1267–68 (2005).

[55] Warren & Brandeis, *supra* note 54, at 193.

[56] *See generally* Daniel J. Solove, *Conceptualizing Privacy*, 90 CAL. L. REV. 1087 1088–94 (2002) (discussing the problems with conceptualizing privacy and suggesting a new pragmatic approach that focuses on privacy problems).

[57] RESTATEMENT (SECOND) OF TORTS, § 652A (1977) ("One who invades the right of privacy of another is subject to liability for the resulting harm to the interests of the other.").

[58] *Id.* § 652C ("One who appropriates to his own use or benefit the name or likeness of another is subject to liability to the other for invasion of his privacy.").

[59] *Id.* § 652E ("One who gives publicity to a matter concerning another that places the other before the public in a false light is subject to liability to the other for invasion of his

publication of private facts,[60] and intrusion.[61] Causes of action based upon privacy torts would be most appropriate where the plaintiff was the subject of online confessions, online gossip, and online insults.

2. Other Torts

Defamation law protects the interests of a person in his or her reputation.[62] To establish liability for defamation, the plaintiff must show that the defendant made a false and defamatory statement that harmed the plaintiff's reputation.[63] Two types of defamation torts exist: libel and slander. Libel is the publication of defamatory statements by printed or written words.[64] Slander is the publication of defamatory matter by spoken words or by any form of communication other than those covered by libel.[65] Defamation-based causes of action would be appropriate where the plaintiff is the subject of online gossip, online insults, and online confessions, provided that the statements made were untrue. Ironically, the wild, juvenile nature of much online discourse may exculpate posters, as the context may indicate that it should not be taken seriously—although it may nevertheless tarnish the reputation of the subject of the online harassment.[66]

In addition, the target of the online harassment may sue for intentional infliction of emotional distress, sometimes referred to as the tort of outrage, by proving that the poster engaged in extreme or outrageous conduct intending to cause severe emotional distress.[67] While the intentional infliction of emotional distress may provide a basis for all kinds of online harassment, it is particularly useful with cyberdeception, which often has a different character from, and occurs more frequently than, offline cases of false identity.

---

privacy, if (a) the false light in which the other was placed would be highly offensive to a reasonable person, and (b) the actor had knowledge of or acted in reckless disregard as to the falsity of the publicized matter and the false light in which the other would be placed.").

[60] *Id.* § 652D ("One who gives publicity to a matter concerning the private life of another is subject to liability to the other for invasion of his privacy, if the matter publicized is of a kind that (a) would be highly offensive to a reasonable person, and (b) is not of legitimate concern to the public.").

[61] *Id.* § 652B ("One who intentionally intrudes, physically or otherwise, upon the solitude or seclusion of another or his private affairs or concerns, is subject to liability to the other for invasion of his privacy, if the intrusion would be highly offensive to a reasonable person.").

[62] *See* Hearst Corp. v. Hughes, 466 A.2d 486, 489–90 (Md. Ct. App. 1983).

[63] RESTATEMENT (SECOND) OF TORTS §§ 558–59 (1977).

[64] *See id.* § 568.

[65] *See id*.

[66] *See supra* notes 2–4 and accompanying text.

[67] RESTATEMENT (SECOND) OF TORTS § 46 (1977) ("One who by extreme or outrageous conduct intentionally or recklessly causes severe emotional distress to another is subject to liability for such emotional distress, and if bodily harm to the other results from it, for such bodily harm.").

3. Crimes

In addition to torts, online threats and/or cyberstalking may also be a crime.[68] Typically, the defendant must have engaged in behavior or a pattern of conduct with the intent to alarm, abuse, or frighten the victim.[69] Acts of cyberterrorism may be criminalized under anti-hacking statutes.[70]

B. The Inadequacy of Existing Remedies

Online harassment is distinct in both the process by which it occurs and the harms that it creates. While existing remedies discussed in the previous section may adequately address offline harassment, they are inadequate to deal with online harassment for several reasons.

First, posting is cheap and easy, which produces two effects with respect to online harassment. Offline publishers often have deep pockets, and the range of their distributive reach correlates with their financial means. On the Internet, however, widespread distribution is available to those without substantial financial resources. Consequently, even where a plaintiff prevails in a civil action against an online harasser, the odds are high that the plaintiff will not be able to recover significant damages.[71]

Furthermore, online harassment affects private individuals in a very public manner by means that were previously infeasible. Because posting is cheap and easy, many forms of online harassment are more likely to involve a nonpublic figure than offline forms of the same conduct. For example, online publication of insults and gossip about nonpublic figures is much more common than publication of insults and gossip about nonpublic figures in traditional media. Unfortunately, because litigation is costly, many private individuals who are the target of online harassment do not have the financial resources to pursue legal remedies. For

---

[68] *See, e.g.*, CAL. CIV. CODE § 1708.7 (West 2009) (describing the tort of stalking, including cyberstalking, where the defendant engaged in a "pattern of conduct the intent of which was to follow, alarm or harass the plaintiff" and the plaintiff "reasonably feared for his or her safety, or the safety of an immediate family member"); CAL. PENAL CODE § 422 (West 2009) (making it a crime for a person "who willfully threatens to commit a crime which will result in death or great bodily injury to another person, with the specific intent that the statement, made verbally, in writing, or by means of an electronic communication device, is to be taken as a threat, even if there is no intent of actually carrying it out" thereby causing a person "reasonably to be in sustained fear for his or her own safety or for his or her immediate family's safety").

[69] *See* CAL. CIV. CODE § 1708.7 (West 2009); CAL. PENAL CODE § 422 (West 2009); *see also* MASS. GEN. LAWS ANN. ch. 265, § 43 (LexisNexis 2002); OHIO REV. CODE § 2917.21(B) (LexisNexis 2005); ALASKA STAT. § 11.61.120 (2007); TEX. PENAL ANN. § 42.07 (Vernon 2008); ALA. CODE § 13A-11-8 (2009).

[70] *See, e.g*, 18 U.S.C. § 1030 (2006) (criminalizing fraud and related activity in connection with computers).

[71] *See, e.g.*, Margolick, *supra* note 2.

example, the female law student plaintiffs in the AutoAdmit case could afford to bring a lawsuit against their aggressors because they were represented at no charge by one of the country's leading litigation firms, and by one of the country's leading intellectual property lawyers.[72] It is unlikely that they would have done so otherwise; although the plaintiffs were seeking monetary damages, they would probably not have received much because many of the defendants were students and/or recent graduates and may have lacked the financial means to satisfy a substantial judgment.[73]

Second, many harassing posts are anonymous. Anonymity removes many of the social controls that may have deterred offenders in the pre-Internet era.[74] Anonymity also reduces accountability and accuracy.[75] Anonymous information is simply not disseminated as easily offline as it is on the Internet. While one may argue that anonymously authored postings are not as credible as identified postings, the mere existence or prevalence of online gossip or online insults may have a negative effect even where such information is refuted or discredited. One study showed that repeated exposure to information made people believe the information was true, even where the information was identified as false.[76] The "illusion of truth" appears to come from increased familiarity with the claim and decreased recollection of the original context in which the information was received.[77]

---

[72] *Id.* The lawsuit has since been settled. *See* Ilana Seager, *Law Graduates Settle Suit*, YALE DAILY NEWS, Oct. 23, 2009, *available at* http://www.yaledailynews.com/news/university-news/2009/10/23/law-graduates-settle-suit/.

[73] *See id.*

[74] *See* DANIEL J. SOLOVE, THE FUTURE OF REPUTATION: GOSSIP, RUMOR AND PRIVACY ON THE INTERNET 140 (2007) (noting "anonymous, people are often much nastier and more uncivil in their speech [because it] . . . is easier to say harmful things about others when we don't have to take responsibility"). Solove adds that a gossiper risks harm to his or her own reputation, as well as the reputation of others: "If a person gossips about inappropriate things, betrays confidences, spreads false rumors and lies, then her own reputation is likely to suffer. People will view the person as untrustworthy and malicious. They might no longer share secrets with the person. They might stop believing what the person says." *Id*. at 140–42.

[75] Justice Scalia made this argument in his dissent in *McIntyre v. Ohio Elections Commission*, 514 U.S. 334, 382 (1995) (Rehnquist, C.J., joined by Scalia, J., dissenting) (noting "a person who is required to put his name to a document is much less likely to lie than one who can lie anonymously" and that anonymity "facilitates wrong by eliminating accountability"); s*ee also* Branscomb, *supra* note 20, at 1642–43 (noting anonymous or pseudonymous postings "relieve[] their authors from responsibility for any harm that may ensue [and that] . . . [t]his often encourages outrageous behavior without any opportunity for recourse to the law for redress of grievances"); SOLOVE, *supra* note 74, at 462–64.

[76] *See* Ian Skurnik et al., *How Warnings About False Claims Become Recommendations*, 31 J. CONSUMER RES. 713, 714 (2005).

[77] *Id.*

Anonymity also reduces the likelihood of nonlegal measures or conciliatory efforts.[78] If one can anonymously submit a post airing a grievance or a claim, one has less incentive to seek out the object of the post to determine its accuracy or to resolve the conflict giving rise to the grievance. Perceived wrongs can be redressed the coward's way, by anonymously posting the rumor or incident for public opprobrium. If the victim of a post is unable to *identify* the poster, he or she is unable to resolve any conflicts or clarify any issues in a nonlegal manner.[79] The victim of online harassment must initiate legal proceedings to unmask the identity of the poster as there may be no other way to negotiate with the poster or respond to the posting, other than by responding via a post.[80] In fact, anonymity removes any opportunity to redress grievances in a nonpublic manner if the Web site sponsor is unwilling to intervene on the victim's behalf. The victim must try to ignore the post (an admirable but perhaps unrealistic effort), react via a responsive post, or initiate an often costly and time-consuming lawsuit, which may draw even more attention to a humiliating or threatening post. As previously mentioned, the lawsuit may ultimately be fruitless because the poster is without significant resources or is a minor.[81] Even if the subject of the post prevails in a lawsuit, posts may remain online and linked to by other Web sites during the drawn-out litigation, causing more emotional harm.

Third, near instantaneous, widespread dissemination and the impossibility of recapturing distributed postings put online harassment injuries in a class by themselves. There is no comparable injury in the offline world because there is no other method of distribution that is as inexpensive, accessible, widespread, and difficult—if not impossible—to retrieve. Online insults, for example, may not be libelous; yet, through their widespread distribution and permanence, they are harmful in a way that offline insults are not. Secrets and gossip have the potential to cause much greater reputational damage when spread online than when shared over a cup of tea among friends. Furthermore, anonymity enables less restrained disclosure as it frees the discloser from the stigma associated with salacious information.

Whether the Internet is different from the offline world, and thereby necessitates different rules, has been a recurring topic of discussion among

---

[78] *See infra* notes 84–86 and accompanying text.

[79] *See infra* notes 84–86 and accompanying text.

[80] *See infra* notes 84–86 and accompanying text; *see also* Caroline E. Strickland, Note, *Applying* McIntyre v. Ohio Elections Comm'n *to Anonymous Speech on the Internet and the Discovery of John Doe's Identity*, 58 WASH & LEE L. REV. 1537, 1539–41 (2001) (noting that without knowledge of online posters' identities, a corporation that is the object of cybersmears has limited options and that, as a result, "Corporation X can only hope to obtain a damages award from the thus far unidentified parties," by filing a lawsuit against "John Doe").

[81] *See supra* note 73 and accompanying text; *see also* Branscomb, *supra* note 20, at 1643 ("Law enforcement officials or lawyers seeking to file a civil suit might not be able to identify an individual to hold responsible.").

academics and commentators.[82] Perhaps the more relevant issue, at least regarding the problem of online harassment, is not whether the Internet is inherently different as a mode of communication, but, rather, whether Internet-related conduct and the effects of such conduct is, and has been, *treated* differently from non-Internet-related conduct. The answer to that is an unequivocal *yes*. Users say and do things on the Internet they would not in the offline world, which is something psychologists refer to as the online "disinhibition effect."[83] Web site sponsors routinely accept anonymous postings, whereas major newspapers generally require at least a contact name and telephone numbers, and often require additional biographical information about the author.[84] Offline gossipmongers typically do not spread their information wearing bags over their heads. The petty and malicious gossip of college students is not typical fodder for national print publications.

Even where anonymity is not an issue because the poster has self-identified, the Internet poses unique challenges that make traditional responses to harassment inadequate. Web site sponsors often disclaim all responsibility for harassing conduct that occurs on their Web sites, and many make no attempt to monitor or control uploaded content.[85] In contrast, if such conduct were to occur on physical property—written on a bathroom wall or posted on a bulletin board in a store, for example—social norms and fear of a lawsuit would compel the store owner to take some sort of action. Distributing false rumors in the physical world is a tort for which the publisher is liable, yet in cases where rumors are spread via the Internet, Web sites are immune from liability under section 230 of the CDA.[86]

---

[82] *See, e.g.*, Frank H. Easterbrook, *Cyberspace and the Law of the Horse*, 1996 U. CHI. LEGAL F. 207, 208 (noting it is not clear whether many features of existing law can be appropriately applied in the cyberrealm); *cf.* Lawrence Lessig, *The Law of the Horse: What Cyberlaw Might Teach*, 113 HARV. L. REV. 501, 502 (1999) (arguing "there is an important general point that comes from thinking in particular about how law and cyberspace connect").

[83] *See* John Suler, *The Online Disinhibition Effect*, 7 CYBERPSYCHOL. & BEHAV. 321, 321 (2004); *see also* John M. Grohol, *Teens, Sex and Technology*, http://psychcentral.com/blog/archives/2009/01/06/teens-sex-and-technology (Jan. 6, 2009).

[84] *See, e.g.*, *Op-Ed Guidelines for the Wall Street Journal*, WALL ST. J., http://www.opinionjournal.com/guidelines (requiring the contact name and telephone number of authors); *Submissions & Contributions*, S.F. CHRON., http://www.sfgate.com/chronicle/submissions (requiring the contact name and telephone number of authors); *Submitting an Article to Op-Ed*, L.A. TIMES, http://www.latimes.com/news/opinion/oe-howtosubmitoped,0,5238591.story (requiring the contact name and telephone number of authors, as well as biographical information).

[85] *See supra* note 9 and accompanying text.

[86] *See* Doe v. MySpace, Inc., 528 F.3d 413, 418–20 (5th Cir. 2008); Carafano v. Metrosplash.com, Inc., 339 F.3d 1119, 1123 (9th Cir. 2003) (stating doubts should be "resolved in favor of immunity"); Goddard v. Google, Inc., No. C 08-2738 JF (PVT), 2008 WL 5245490, at *2 (N.D. Cal. Dec. 17, 2008) (noting courts "consistently have held that section 230 provides a 'robust' immunity"); Barrett v. Rosenthal, 146 P.3d 510, 529 (Cal.

The remedies currently available require a victim of online harassment to file costly, time-consuming, and often fruitless lawsuits. Although this may be a problem in the physical world, it is a greater problem in the virtual world because of the unique aspects—ease of publication, section 230 immunity for Web sites, anonymity, widespread distribution, and lack of control—of Internet publication.

Online harassment can be combated by changing the roles that Web site sponsors currently play and by imposing tort liability on those who fail to meet certain expectations. Web site sponsors maintain a proprietary interest in their Web sites, and we should expect them to conform to the standard of conduct expected of other proprietors.[87] The interpretation of that standard, however, should recognize the differences between online and offline businesses. In other words, while we should expect proprietors to conduct their businesses with reasonable care, what constitutes reasonable care should take into consideration the differences between online and offline businesses. The proposals set forth in Part IV provide guidance as to what might constitute reasonable care on the part of Web site sponsors.

IV. PROPOSALS TO ADDRESS THE PROBLEM OF CYBERHARASSMENT

Given the harm created by nearly instantaneous widespread dissemination, the lack of editorial controls, and other obstacles to publication—and perhaps most significantly, the irretrievability and permanence of the effects of online harassment—the primary objectives of the proposals set forth in this section are deterrence and prevention. Tort remedies and criminal prosecutions provide scant comfort to victims of online harassment who lack the resources to pursue available remedies and/or wish to avoid further publicity.[88] The remedies also often exacerbate the emotional trauma of having had personal details or images released to an audience of millions. The permanence of Internet distributions also makes rehabilitation much more difficult. One undergraduate student stated it was a challenge to continue his new life as a college student after he was identified by name as having appeared in a pornographic movie in a post on the Juicy Campus

---

2006) (noting section 230 "does not permit" Internet service providers or users to be sued as "distributors").

[87] Black's Law Dictionary defines "proprietor" as "[a]n owner, esp. one who runs a business." BLACK'S LAW DICTIONARY 1339 (9th ed. 2009).

[88] Solove raises many of the same concerns expressed in this Article. His proposals focus on broadening the current definition and application of existing tort remedies to deter future instances of cyberharassment. *See* Solove, *supra* note 74, at 113. He also introduces remedies, such as alternative dispute resolution measures, that would limit the impact of cyberharassment. *Id.* at 124. Although I agree with many of Solove's proposals, my proposals focus more on prevention of cyberharassment through primarily nonlegal measures.

Web site.[89] The post also linked to a Web site that showed him engaging in explicit sexual acts with other men.[90]

These proposals recognize that some forms of online harassment have the potential to cause more harm than others. They also take into account that at least some forms of online harassment potentially have social value, including expressive value, whereas other forms of online harassment do not. These proposals consider and balance the competing interests of both the poster and the subject of the post.

The proposals focus primarily on two aspects of Internet conduct that differentiate online harassment from physical-world harassment. The first is anonymity. While anonymous speech occurs in the physical world, it is more difficult to accomplish and less likely to occur than online. While anonymity has benefits—in particular for minority groups who may, for economic or social reasons, lack other forums for communication—it also has serious drawbacks. As discussed in Part III(B), anonymity may remove incentives for self-regulating behavior so that an anonymous poster may be more inclined to post damaging material. A poster may also be willing to post more vicious or less discreet information if he or she can do so anonymously. Disassociative anonymity is one of the factors causing online disinhibition.[91] Anonymous users feel less vulnerable about being frank and do not feel responsible for their online conduct.[92]

Finally, the notion of anonymity itself is misleading. In many cases, the identity of a user is accessible, even if such accessibility requires some effort. The government or a party to a lawsuit can subpoena user identification.[93] In addition, the Web site sponsor often requires user registration, thereby identifying the poster internally, even if users are unaware of the poster's identity.[94] This Article's proposals thus make plain for the user that anonymity is not permanent or secure, and may encourage users to reconsider impulsive, regrettable behaviors without overly restricting considered and desired communications.

My proposals also advocate a more responsible role for Web site sponsors. Because of the private regulatory nature of the Internet,[95] Web site sponsors are in

---

[89] Richard Morgan, *A Crash Course in Online Gossip*, N.Y. TIMES, Mar. 16, 2008, at ST. 7.

[90] *Id.*

[91] Suler, *supra* note 83 (noting that "anonymity works wonders for the disinhibition effect").

[92] *Id.*

[93] *See supra* notes 2–5 and accompanying text (discussing the AutoAdmit case).

[94] *See* Branscomb, *supra* note 20, at 1643 ("Many providers of computer-mediated facilities do not permit genuine anonymity. They keep records of the real identity of pseudonymous traffic so that abusers can be identified and reprimanded."). Branscomb, however, notes there is a trend toward using "anonymous remailers" who "provide a guarantee that messages cannot be traced back to their sources." *Id.*

[95] *See* Nunziato, *supra* note 18, at 1116 (noting the "vast majority of speech on the Internet today occurs within private places and spaces that are owned and regulated by private entities").

the best position to address the problem of online harassment. Web site sponsors have borrowed the rhetoric of free speech as though they were public forums while taking full advantage of their sites as private businesses.[96] As a matter of fairness and consistency, Web site sponsors should have a duty to take reasonable steps to prevent tortious and criminal conduct on their Web sites, at least in certain circumstances. These reasonable steps should include policies to deter online harassment that incorporate at least some of the proposals set forth in this Article.

A. Contractual and Architectural Constraints

One way Web sites may prompt posters to reconsider their postings is by implementing contractual and architectural restraints, many of which already exist on commercial Web sites.[97] As many scholars have explained, the way choices are presented influences their selection or nonselection.[98] Object design or architecture

---

[96] As Dawn Nunziato notes:

> Private regulation of speech on the Internet has grown pervasive, and is substantially unchecked by the Constitution's protections for free speech, which generally apply only to state actors' regulations of speech. At an earlier stage of the Supreme Court's First Amendment jurisprudence, such private speech regulations might have been subject to the dictates of the First Amendment under the state action doctrine. The Supreme Court, however, has substantially limited the application of the state action doctrine in past decades, and courts have been unwilling to extend this doctrine to treat private regulators of Internet speech as state actors for purposes of subjecting such regulation to First Amendment scrutiny.

Id.

[97] While some of the contractual restraints may prove to be unenforceable if the poster is a minor, they may nevertheless have a deterrent effect on undesirable behavior. Furthermore, a court might enforce a Web site's terms of service against a minor. *See* A.V. v. iParadigms, 544 F. Supp. 2d 473, 480–81 (E.D. Va. 2008) (enforcing the terms of a clickwrap agreement against minor plaintiffs and stating that plaintiffs could not "use the infancy defense to void their contractual obligations while retaining the benefits of the contract").

[98] *See* DONALD A. NORMAN, THE DESIGN OF EVERYDAY THINGS 141–218 (1988) (discussing the influence of product design upon consumer behavior and use); RICHARD H. THALER & CASS R. SUNSTEIN, NUDGE: IMPROVING DECISIONS ABOUT HEALTH, WEALTH, AND HAPPINESS 81–100 (2008) (citing social studies to explain how choice architecture can be used to improve decision making); KIM VICENTE, THE HUMAN FACTOR: REVOLUTIONIZING THE WAY PEOPLE LIVE WITH TECHNOLOGY 65–280 (2004) (discussing how technological advancements must be designed with human limitations in mind). In the context of software and the Internet, see LAWRENCE LESSIG, CODE AND OTHER LAWS OF CYBERSPACE 7–8 (1999) (explaining why the architecture of cyberspace matters); James Grimmelmann, Note, *Regulation by Software*, 114 YALE L.J. 1719, 1721–45 (2005) (noting the ways that regulation by software is, and is not, like physical architecture); Joel R. Reidenberg, *Lex Informatica: The Formulation of Information Property Rules Through*

along with human foibles and limitations influence decisions and object use (or misuse).[99] The contractual and architectural constraints proposed in this Part create structural barriers to speech without unreasonably restricting it. In other words, the constraints may serve in their modest way the purposes of time, place, and manner restrictions, as well as the purposes of physical, logistical, and normative barriers imposed upon speakers in the physical world.

1. Manifesting Assent to Web Site Policies

Web site sponsors can require posters to register with the Web site before gaining the ability to post comments. Although posters can easily create e-mail addresses and use false information, having to go through the motions of doing so may slow down the posting process or cause posters to reconsider their communications. As part of the posting process, a poster may be reminded of the Web site's policy against online harassment.[100] The poster may be asked to click "I agree" to the terms of the policy. The physical act of consent may remind the poster of the legally binding nature of agreement. In the alternative, or in addition to expressing agreement to the terms of the Web site's online harassment policy, the poster may be asked, "Are you sure you want to post this?" A simple question requiring a pause may be annoying to some, but it may also cause posters to consider whether they really want to continue. Web site sponsors can also institute comment policies or moderate user comments.

2. Indemnification for User Misconduct

Additionally, Web site sponsors could discourage online harassment by requiring that all users contract to indemnify the sponsors from any harm the users cause. Part V advocates the imposition of proprietorship tort liability upon Web site sponsors for foreseeable harm caused by third parties. Web site sponsors, in turn, can reduce their risk of tort liability by contracting for indemnification with their users. To ensure enforceability, the agreement should be concise,

---

Technology, 76 TEX. L. REV. 553, 555 (1998) ("Technological capabilities and system design choices impose rules on participants. The creation and implementation of information policy are embedded in network design and standards as well as in system configurations."); Rajiv C. Shaw & Jay P. Kesan, *Deconstructing Code*, 6 YALE J. OF L. & TECH. 277, 279 (2003) (explaining how "code is not neutral and apolitical, but instead embodies the values and motivations of the institutions and actors building it"); *see also* JONATHAN ZITTRAIN, THE FUTURE OF THE INTERNET—AND HOW TO STOP IT 228–29 (2008) (discussing a form of "reputation bankruptcy" as an example of a design choice that Web site intermediaries could adopt to capture "the nuances of human relations far better than our current systems"). Zittrain adds that "online intermediaries might well embrace such new designs even in the absence of a legal mandate to do so." *Id*. at 229.

[99] As Joel Reidenberg has observed, "Even user preferences and technical choices create overarching, local default rules." Reidenberg, *surpra* note 98, at 555.

[100] Of course, this would require that the Web site have such a policy.

understandable, and conspicuous. Furthermore, the user should be required to manifest assent by clicking, rather than burying the terms in an interior "terms of use" page. Requiring active assent may make users realize that a Web site is serious about enforcing its anti-harassment policies and encourage users to consider the legal repercussions of their actions.

3. Community Controls

In addition, the Web site might incorporate user-generated controls on content. For example, some Web sites incorporate "report abuse" buttons to enable visitors to report offensive content or abusive conduct.[101] Wikipedia enables users to update and delete content placed by others, and it has reportedly changed its policy so that new and anonymous users must have their content "flagged," or approved by registered, reliable users.[102] Craigslist incorporates an easy way to flag certain posts by categorizing the violation and enabling the user to click on the upper right-hand side of each listing.[103] Amazon and eBay enable users to rate other users.[104] All of these controls can be incorporated on other Web sites as well. A message board can have users rate the quality of a particular poster for the benefit of newcomers. The online version of the San Francisco Chronicle, for example, enables readers to click on an icon to indicate a "thumbs up" or "thumbs down" in rating a poster's comments.[105] Users can also report offensive posts and request that such posters be banned from the Web site.

4. Default to Identified Postings

Another architectural control that Web sites can implement is a default to identified postings rather than anonymous postings. Currently, much of Internet communication is structured to facilitate anonymous postings and to accord each posting equal weight. Instead, communication could be structured to default to

---

[101] *See, e.g.*, *Terms and Conditions*, S.F. CHRON., http://www.sfgate.com/pages/termsandconditions (last visited Sept. 1, 2009) (incorporating "report abuse" buttons to report offensive and abusive conduct). A Web site security group recently recommended that Web sites aimed at consumers incorporate such buttons on their sites. *See* David Neal, *Security Group Calls for 'Report Abuse' Button on Web Sites*, June 1, 2009, http://www.v3.co.uk/vnunet/news/2243285/isaf-pushes-security-button.

[102] Noam Cohen, *Wikipedia May Restrict Public's Ability to Change Entries*, http://bits.blogs.nytimes.com/2009/01/23/wikipedia-may-restrict-publics-ability-to-change-entries (Jan. 23, 2009, 17:46).

[103] *See* craigslist, http://www.craigslist.org (last visited Sept. 1, 2009).

[104] *See* eBay, *Feedback Forum*, http://pages.ebay.com/services/forum/feedback.html (last visited Sept. 1, 2009); Amazon, *Rating Your Amazon Marketplace Seller*, http://www.amazon.com/gp/help/customer/display.html?nodeId=537806 (last visited Sept. 1, 2009).

[105] *See* The San Francisco Chronicle, http://www.sfgate.com (last visited Sept. 1, 2009).

postings that identify the poster, unless the poster opts to post anonymously by clicking out of the default each time the user tries to post a message, in much the same way that companies currently require customers to opt out of receiving marketing information. It would be most effective if the ability to opt out required the user to navigate through another Web page, rather than merely checking a box on the same page. Of course, some posters would continue to falsify their registration information or take the extra step to opt out of identification, but some might not. The point is not to make identified postings mandatory, but to make identified postings easier than slightly more burdensome anonymous postings.

5. "Cooling Period"

A Web site sponsor can incorporate hurdles or procedures to slow down the posting process, encouraging posters to more carefully consider what they say before they press "Send." Because anonymity and the ease and pace of the Internet may encourage impulsive behavior, one way to curb such behavior is to require a "cooling period." A poster might be required to wait before a message or image is posted to a Web site. During this cooling period, the poster may choose to edit or remove the message or image from the posting "queue." Some may object that instituting a cooling period will harm spontaneous discussion on message boards. This harm can be minimized by imposing a cooling period that reflects the type of harassment likely to occur on the Web site. Blog sites on political topics, for example, may require a shorter period of time, say ten minutes, whereas social networking sites may require a twenty-four-hour waiting period. Alternatively, a different waiting period may be instituted where the poster wishes to remain anonymous. Those users who choose to identify themselves may have a shorter waiting period, or no waiting period at all, whereas anonymous posters may be subject to a longer cooling period. Any waiting period at all encourages further reflection, which may have the additional benefit of better written and more thoughtful posts.

6. Warning Notices

Notices may also deter misconduct. A notice may inform a poster of the legal consequences of his or her actions. Some posters may be ignorant of what constitutes tortious or criminal behavior. Simply knowing that a defamatory or threatening post subjects the poster to a civil lawsuit may be enough to deter a poster who might not otherwise realize—either because of ignorance or because the issue is not at the mind's forefront at the time of posting—the risks of his or her conduct. A reminder that a posting may have legal repercussions may prompt a poster to soften the language or reconsider the message.

A recent study illustrates the effectiveness of warning notices.[106] Researchers created a MySpace page for "Dr. Meg" that identified her as a doctor.[107] The researchers then found MySpace users who identified themselves as eighteen to twenty years of age, and who discussed sexual activity and substance use on their publicly viewable pages.[108] "Dr. Meg" sent these users a note informing them of the risk of disclosing personal information along with a link to a Web site about sexually transmitted diseases.[109] Three months later, the researchers learned that 42.1 percent of the MySpace pages had been changed (either by enhancing privacy settings or by deleting the references to sex and/or substance use) compared with 29.5 percent in the control group.[110]

In addition to notifying the poster of what constitutes potentially criminal and tortious activity, the poster should be informed of the Web site's policies governing user activity, especially because many such policies restrict more types of activity than are prohibited by law. This type of reminder is particularly important for social networking sites where users routinely violate policies that forbid harassing or annoying other members.

Notices could also inform posters of the circumstances under which their identities may be revealed. Some posters may not know, or may not consider at the time of posting, that "anonymity" is rarely secure and inviolable.[111] Posters' identities are usually known by the Web site sponsors and by Internet service providers.[112] Poster identity may be revealed where a lawsuit has been filed pursuant to a subpoena, even where the Web site and the poster wish to maintain anonymity.[113] In some cases, Web site policies may permit unmasking users under certain conditions, a few of which are suggested in the next section. Other posters may also reveal the identity of anonymous posters. For example, an anonymous blogger was recently identified as a law professor by another poster on a popular Web site.[114] Informing posters of the tenuous nature of anonymity may cause some to modify their postings. To illustrate, it is unlikely that the students who posted offensive comments about female law students on the AutoAdmit message board

---

[106] Megan A. Moreno, *Reducing At-Risk Adolescents' Display of Risk Behavior on a Social Networking Web Site: A Randomized Controlled Pilot Intervention Trial*, 163 ARCHIVES OF PEDIATRIC & ADOLESCENT MED. 35, 35–41; *see also* Eric Nagourney, *A Note to the Wise on MySpace Helps*, N.Y. TIMES, Jan. 6, 2009, at D6 (discussing teenagers posting highly personal information that is accessible to future employers or online predators).

[107] Moreno, *supra* note 106, at 36.

[108] *Id.*

[109] *Id.* at 37.

[110] *Id.* at 38.

[111] *See supra* notes 93–94 and accompanying text.

[112] *See supra* notes 93–94 and accompanying text.

[113] *See supra* notes 2–6 and accompanying text (discussing the AutoAdmit case).

[114] Debra Cassens Weiss, *Netiquette Debate Erupts Over Law Professor's Outing as 'Publius' Blogger*, A.B.A. JOURNAL.COM, June 9, 2009, http://www.abajournal.com/news/netiquette_debate_erupts_over_law_profs_outing_as_publius_blogger/print/.

would have done so if they had realized that their true identities might be revealed in the course of a lawsuit. They would have likely reconsidered how to phrase their posts, or they might have declined to post at all given the damage to their personal and professional reputations.

To be most effective, warnings and other notices should be concise and in plain English to be comprehensible to most users.[115] It may be helpful for notices to include examples of what constitutes each type of prohibited conduct. Finally, notices should appear at the time of posting, rather than as a general message on the Web site or tucked in an interior page.

B. Ameliorating Anonymity's Negative Effects

One of the problems associated with anonymity on the Internet is that it minimizes posters' accountability for their actions. Anonymity encourages a lack of accountability because posters may feel more comfortable posting comments if their identities can remain hidden. There are, however, valid arguments in favor of anonymity.[116] Stripping all posters of anonymity to curb online harassment is an overbroad measure because it threatens to stifle many socially beneficial forms of communication. Members of subcultures or minority social, racial, religious, and/or political groups may fear repercussions for posting unpopular views or for expressing beliefs, desires, or thoughts that do not conform to mainstream values or norms. An atheist may post remarks that question God's existence. A teenage boy may seek support regarding his sexuality. A girl may ask for advice regarding an abortion. Anonymity enables all of them to share and receive important information. Given that one of our culture's values is the protection of minority views, an absolute ban on anonymity is, for this reason, not encouraged.

Certain types of conduct merit more identity protection, however, than others. As previously discussed, anonymity may facilitate discussion for a variety of reasons.[117] One of the most important is that it enables those afraid to speak to seek advice, support, and information from others without fear of repercussion. In some cases, however, anonymity is not useful because it enables and facilitates online harassment, often of members of the very same minority or disempowered groups.[118] Currently, the only way a victim of online harassment can unmask the

---

[115] *See* Robert P. Bartlett III & Victoria C. Plaut, *Blind Consent? A Social Psychological Investigation of Non-Readership of Click-Through Agreements* (forthcoming 2009), *available at* http://repositories.cdlib.org/cgi/viewcontent.cgi?article=1233&context=berkeley_law_econ (finding that shorter form click agreements in a more readable format appeared to make contract terms more salient and meaningful).

[116] For a comprehensive discussion of the costs and benefits of anonymous speech, see Lyrissa Barnett Lidsky & Thomas F. Cotter, *Authorship, Audiences, and Anonymous Speech*, 82 NOTRE DAME L. REV. 1537 *passim* (2007).

[117] *See id.*

[118] *See* Christopher Wolf, *Racists, Bigots and the Law on the Internet*, ANTI-DEFAMATION LEAGUE, http://www.adl.org/Internet/Internet_law1.asp (last visited Sept. 1, 2009) (explaining how the Internet is "a relatively cheap and highly effective way for hate

identity of an anonymous poster is to file a lawsuit. In most cases, however, the process is time consuming and costly. Because it is time consuming, the damaging information remains online longer. The costliness of litigation is aggravated by the likelihood that the harassers are judgment-proof. Victims are consequently left without recourse. Therefore, one solution is to permit victims of certain types of online harassment to unmask harassing posters without filing lawsuits.

1. Easy Unmasking of Anonymity

The "easy unmasking" of anonymity proposed here is limited to situations where all of the following factors are present: the victim of the online harassment has been identified in a posting; the victim is a nonpublic individual; the victim has signed an affidavit swearing that he or she is the individual identified in the posting; and the victim sets forth facts establishing why easy unmasking is warranted. These limitations aim to limit easy unmasking to situations where the posts do not involve matters of legitimate public interest. The downside to these limitations is that there may be victims of online harassment (i.e., public officials) who are unable to easily unmask their anonymous harassers. Those individuals, however, may still seek to strip anonymity by filing a lawsuit and seeking recourse under the currently available remedies.[119]

Several reasons support easy unmasking of a cyberharasser. The first is deterrence. If the barriers for removing anonymity are lowered, and the harasser is aware of that, he or she may be less inclined to post harassing information. The second is redress. If the victim knows the harasser's identity, the victim can more effectively respond to the posted information and assess the credibility of the threat. Anonymous threats hover ominously online and permit the victim to imagine the most terrible culprits. A female law student who was the target of online threats on the law school admission message board, AutoAdmit, stated, "I . . . felt kind of scared because it was someone in my community who was

---

groups as diverse as the National Alliance and the Ku Klux Klan, as well as anti-Semites, right-wing extremists, militia groups, and others to propagate their hateful ideas"); *see also* Andrew Chin, *Making the World Wide Web Safe for Democracy: A Medium-Specific First Amendment Analysis*, 19 HASTINGS COMM. & ENT. L.J. 309, 310 (1997) (observing that "[t]o the extent that the Web's free market of homepages and links amplifies the voices of the powerful and silences the powerless, impoverishing public debate, corrective policy measures should be constitutionally favored"); *Democracy Gone Wild: Hate Speech Infests Online Versions of Local Daily Newspapers*, PASADENA WKLY., June 12, 2008, at 8 (describing the hateful, racially charged posts of "Viking Knight" on newspaper Web sites); Valenti, *supra* note 43, at 16 (noting that on some online forums "anonymity combined with misogyny can make for an almost gang-rape like mentality"). For an extensive discussion of how online anonymous mobs threaten the online speech of traditionally disadvantaged groups, see Citron, *supra* note 12, at 68–84.

[119] *See* discussion *supra* Part III.A.

threatening physical and sexual violence and I didn't know who."[120] In some instances, those fears are justified. In others, they may not be. Enabling victims of online threats to put a face on their tormentors helps the victims determine what they should do next, whether it is filing a police report or calling an underage harasser's parents. Harassers may then feel social pressure to stop the harassing behavior without judicial intervention.

Some may argue that permitting the unmasking of the harasser subjects the harasser to attacks by the victim. It is important to keep in mind that easy unmasking would only be permitted where personal information about the victim, including the victim's identity, was revealed online. Easy unmasking would not be permitted in situations where the victim was not identified to the public. Thus it would not occur in situations where one was speaking about an issue or problem, where the information was conveyed in generalities, or where the victim was not identified. Furthermore, easy unmasking would not be permitted where the gossip pertained to a company or business entity, or where the individual was a public figure.[121] The concern about unmasking harassers in this context is then puzzling because the victim is only receiving the same type of information that the harasser felt comfortable revealing to the public about the victim. If the harasser feels it is acceptable to release to the public personal, identifying information about the victim, then the victim should be entitled to identifying information about the harasser. Turnabout is fair play and may reinforce the social norms that currently exist in the offline world. Although backbiting and gossip exist everywhere, in most cases the individual spreading the gossip must deal with the consequences of doing so. The gossiper develops a reputation for reliability or misinformation and may be sought out or shunned for the gossip. On the Internet, however, credibility is detached from identity where the gossiper's identity is unknown. An unmasking policy enables a victim of online gossip to respond by revealing critical information about the harasser, such as ulterior motivations, which may undermine the harasser's credibility and thereby minimize the damage from the online harassment. In some situations, such as where the victim and the harasser occupy the same social milieu, such as attending the same school or living in the same neighborhood, an unmasking helps redress the harassment by shaming the harasser. For example, in the AutoAdmit case, the degrading posts affected the academic performance and emotional well-being of the female subjects; the posters, on the other hand, continued about their daily lives comparatively unaffected.[122] Easy unmasking would have allowed these female law students to socially shame their classmates, and would have made it more difficult for some of the posters to continue their messages unchecked. Some of the posters whose

---

[120] Denis Cummings, *Anonymous AutoAdmit Posters to Be Revealed in Court*, FINDINGDULCINIA, Aug. 4, 2008, http://www.findingdulcinea.com/news/technology/July-August-08/Anonymous-AutoAdmit-Posters-to-be-Revealed-in-Court.html.

[121] Of course, this would not foreclose the business or public figure's ability to seek recourse under existing legal remedies.

[122] *See* Margolick, *supra* note 2.

identities were revealed as part of the lawsuit apparently had never even met the women.[123] Easy unmasking would have demonstrated that these posters' comments were fabricated or unfounded and thus, would have reduced their negative impact.

Of course, an easy unmasking policy is unavailing where the poster is the Web site sponsor itself (such as an anonymous blogger)[124], or where the poster has used an anonymity service. But it may reduce some instances of online harassment where the poster has a reputation it wishes to preserve, or where the poster desires to post in a "truly anonymous" manner but does not know how to do so.

2. Stigmatizing Anonymity

For easy unmasking to be effective, the Web site must have an effective registration process. Many Web sites require posters to register their e-mail addresses. Other times, posters can be identified through their Internet protocol addresses. In some cases, however, a poster may use an anonymity provider or remailer using a forged identity, thus becoming "truly" anonymous. The Web site sponsor can deal with truly anonymous posters in one of several ways. It can ban truly anonymous posters from the Web site altogether. It can monitor the content from truly anonymous posters more closely, or require a longer posting time. It can also segregate anonymous postings to minimize their impact or reduce their ability to be searched.

One of the problems with anonymous postings is that readers are unable to assess the credibility of the poster. The current default for Internet postings seems to be anonymity. Changing the default to identified postings may make anonymous postings seem less credible. A poster continues to have the option of remaining anonymous; however, his or her postings can be segregated to the bottom of the message board or otherwise identified as written by someone who wished, for whatever reason, to remain anonymous. Message boards might even post a notice preceding the anonymous messages that underscores the possibility that they may lack authenticity or credibility. Web site sponsors could deprive anonymous posters of unique names, forcing them to identify only as "Anon 1," "Anon 2," etc., thus giving their posts less of a "headline" and no catchy alias without depriving them of a communication forum. For example, the AutoAdmit posters used juvenile pseudonyms such as "playboytroll," "Pauliewalnuts," "Whamo," and "Spanky."[125] Depriving such posters of fanciful user names may reduce the online disinhibition effect. After having his identity revealed, "Whamo" claimed, "I

---

[123] *Id.* (noting that one of the students was an undergraduate at the University of Iowa and another a Seton Hall graduate.)

[124] The ISP, however, may be required by a court to reveal the blogger's identity. *See* James Bone, *Rude Blogger Is Unmasked by Model*, THE TIMES (London), Aug. 19, 2009, at 8 (reporting that a New York supreme court judge ordered Google to reveal the identity of an anonymous blogger so plaintiff could file a defamation lawsuit).

[125] Complaint at 3, Doe I v. Ciolli (D. Conn. 2007), *available at* http://online.wsj.com/public/resources/documents/aaComplaint.pdf.

didn't mean to say anything bad . . . . I said something really stupid on the . . . internet, I typed for literally, like, 12 seconds, and it devastated my life."[126]

Finally, as previously suggested, the Web site may be set up to allow other users to "rate" the quality and credibility of an anonymous user's postings, putting other visitors on notice regarding the veracity or reliability of that particular anonymous user's postings.

C. Notice and Takedown of Certain Postings

Because of the volume of traffic on many Web sites,[127] prescreening is impracticable. Given both the quantity of postings as well as the nature of posts (which are often subjective or difficult to verify), Web site sponsors are ill-equipped to determine the lawfulness of content even after it has come to their attention. Yet, in certain cases, to require Web site sponsors to take down certain posts upon request would not impose an undue burden upon them. This Section argues that Web site sponsors should automatically remove content upon request in three situations: where the request is made by the original poster; where the post is a digital image of a naked person and the takedown request comes from the subject; and where the post is a digital image of a minor and the takedown request comes from the subject's legal guardian.

1. Takedown Request by Original Poster

As previously discussed, online postings are often made in a heightened emotional state. In some cases, the poster may regret having made an online rant about another individual. The Web site sponsor should be required to remove the post upon request of the original poster. One alleged poster to a popular social networking Web site claimed that she posted information about her former partner that she later regretted.[128] She claimed that the Web site refused to remove the post even after repeated requests.[129] A failure to take down the original post upon

---

[126] Margolick, *supra* note 2.

[127] Facebook, for example, reportedly has more than 200 million unique users. *See* Michael Learmonth, *Facebook Crushing MySpace in Traffic*, ADVERTISING AGE (2009), http://adage.com/digital/article?article_id=134062. MySpace reportedly has 100 million unique users. *Id*.

[128] *See* Cindy English, *Don't Date Him Girl! The Lawsuit . . .* , http://www.cheating ways.com/cheaters/dont-date-him-girl-the-lawsuit (Apr. 28, 2007) ("They froze my account and will not delete the poosting after i emailed 10 times for them to get rid of it. Yes I wrote the posting when i was hurt, angry, sad, I was a mess and i wanted him to hurt as much as I was. We are back together and this website is the only thing that is standing in our way of moving forward. Any suggestions on how to get this posting removed?????? I dont really have the money for an attorney but itf it comes down to it i wll have to do it but is asking them to remove a posting to much? They froze my account and left the posting! Crazy!!!) (comment as originally posted by "Jesika").

[129] *Id.*

request should constitute unreasonable conduct. The Web site sponsor may be ill-positioned to verify the accuracy of posted content, but the poster is not. The poster may uncover additional information that makes the original post misleading or false, or the poster may have had time to reconsider what was originally posted. Unfortunately, the poster is often unable to remove the post without the Web site sponsor's cooperation. To require Web site sponsors to remove content upon request of the poster does not require Web site sponsors to prescreen or to make subjective determinations of content accuracy. Furthermore, a Web site sponsor can redress the problem of repeat repentant posters by banning them from the site.

2. Takedown of Two Types of Digital Images (Nude Individuals & Nonpublic Figure Minors)

Digital images and videos arguably have the potential to cause the greatest harm to victims of online harassment. Images tend to stick in the minds of viewers. The popular perception is that pictures do not lie and that one picture is worth a thousand words.

On the contrary, images can distort the truth by presenting only part of the story. They can be digitally altered, or they may capture an image without its context, thus subverting its meaning. They can also expose and identify an individual in a way that mere words cannot, thus creating a greater danger to privacy and security.

In many cases, publication of images has social value. They may create an emotional impact that words alone cannot convey. The social benefit of images should be weighed against the unique harmful effects of the Internet. Given the harm of widespread simultaneous and permanent distribution, two types of images should be outright prohibited without written consent. The first category is images of nonpublic figure minors. Images of nonpublic minors[130] should not be uploaded to publicly accessible Web sites without the written consent of their legal guardians. The second category is images of nude individuals who are identifiable.

[130] Although minors who are public figures may suffer the same negative emotional consequences, they are arguably better prepared to deal with widespread recognition and notoriety. The public also has a more legitimate "right to know" where the image is of a public figure. Thus, although I may personally wish to extend the takedown upon request measure to images of children of public figures, I recognize that such an application likely would be unacceptable under U.S. laws. By contrast, in many European countries, the images of children of public figures cannot be published without parental consent. *See, e.g.*, Stephen Howard, *Rowling Wins Child Privacy Case*, DAILY MAIL, May 8, 2008, at 12 (describing author J.K. Rowling's suit for privacy violations stemming from covert, long-lens photographs of her toddler son); Alex Kingsbury, *Washington Whispers, Photo of Obama and Spain's First Children Causes a Stir*, U.S. NEWS & WORLD REPORT, Sept. 25, 2009 (noting that privacy conventions in Spain prevent publication of photos of politicians); John Moore, *Photo Oops: U.S. Posts Pic of Spain's Goth First Daughters*, ROCKY MTN. IND., Sept. 26, 2009 (noting that under Spanish law, the prime minister can prevent the media from publishing photos of his children).

Images of identifiable subjects who are completely or partially nude (i.e., the breasts, buttocks, and genitalia of a female subject and the buttocks and genitalia of the male subject) should not be permitted to be uploaded to public Web sites without the written consent of their subject.

Unauthorized postings of either type of image should be subject to immediate takedown after notice. Consents should be filed and maintained with the Web site sponsor for at least one year after the digital image has been removed from the Web site. Unlike other user-supplied content, to require Web site sponsors to take down these two types of images does not require them to make difficult subjective decisions. Whether a person is nude is not difficult to determine. Determining whether a person is younger than eighteen by looking at an image is more difficult. The burden on the Web site sponsor, however, is slight, and the sponsor in close cases might simply take down the image upon request of the individual or guardian, or ask for verification of the individual's age.

As a recent study indicates, the brain continues to develop during the teenage years.[131] During this period, the frontal cortex, or the "thinking" part, of the brain grows and synaptically prunes itself.[132] The prefrontal cortex also undergoes change, which means that the part of the teenage brain responsible for controlling emotions and empathy is not yet where it will be in a few years.[133] The video of the "Star Wars Kid" illustrates how even nonsexual images of minors can be used to cruel effect. A fourteen-year-old boy made a video of himself swinging a golf ball retriever around as if it were a lightsaber.[134] His classmates uploaded the video to a video-sharing Web site, where it spread virally.[135] The video remains popular and is often accompanied by abusive comments such as "what the hell is going through this kids mind, this kid must take it up the butt every single night," "he is a fat nerd faggot kid that fights like a loser," and "sad retarded fat kid. seriously what was he thinking the loser."[136]

Children are more emotionally vulnerable than adults to cruel behavior, and their peers are more likely to engage in it than are adults. Children have not yet developed a social and professional reputation to counter a negative online image. Furthermore, most children do not yet have the maturity and fortitude to ignore abusive comments accompanying embarrassing or cruel posted images. For example, after becoming the object of online scorn and ridicule, the "Star Wars kid" dropped out of school and enrolled in a children's psychiatric ward.[137] Given

---

[131] *See* Steve Connor, *The Teenage Brain: A Scientific Analysis*, THE INDEPENDENT, Nov. 5, 2006, at 8.

[132] *Id.*

[133] *Id.*

[134] *See* Oliver Moore, *'Star Wars' Kid Named Most-Seen Clip on Net*, GLOBE & MAIL, Nov. 28, 2006, at A3.

[135] *Id.*

[136] *Star Wars Kid*, YOUTUBE, http://www.youtube.com/watch?v=HPPj6viIBmU (last visited Sept. 1, 2009).

[137] *Star Wars Kid Files Lawsuit*, Wired News Report, July 24, 2003, *available at* www.wired.com/culture/lifestyle/news/2003/07/59757.

a Web site's lack of expressive interest, it should immediately remove an image of a nonpublic minor upon the request of his or her legal guardian.[138]

The prohibition against these two types of images is not as draconian as it might seem. The images would be permissible and uploadable with authorization from the subject of the image (or his or her legal guardian). The Web site would not be required to respond until *after* a takedown request has been made. Many news publications and Web sites already have special policies to address children's privacy and the publication of nude images[139] and the proposal simply mirrors existing social values. In modern American society, people don't walk around in public nude and most people don't want strangers to see them in the buff. Similarly, our society understands that children are more vulnerable than adults and thus require greater protection and paternalism. Furthermore, with the use of photo editing tools, the poster can easily crop out the prohibited figures from otherwise permissible images, such as a group photograph. This proposed prohibition does not prevent the capturing of the image, only its distribution on the Internet. A photographer could still take pictures of children at the park and sell them or publish them in a book; he or she could not, however, post them to a publicly accessible Web site without the consent of the children's guardians.

V. INCREASING WEB SITE ACCOUNTABILITY

Many types of online harassment might be curtailed or prevented if we altered our expectations of Web site sponsors. Although debate continues to rage regarding whether Web sites should be treated as tangible (real or personal) property,[140] legal duties and social norms and values govern the sense of responsibility that most business owners feel regarding the conduct of patrons on their physical property. Yet the legal duties and social norms governing the responsibility of Web site sponsors over the conduct of their users is still evolving

---

[138] The third-party poster can contest removal on First Amendment grounds, but the image should not remain online during the adjudication process.

[139] *See, e.g.*, *Roanoke Times News Standards and Policies*, ROANOKE TIMES, http://www.roanoke.com/newsservices/wb/xp-59614 ("We do not have specific moratoriums against the publication of any type of accurate news picture. Pictures that show extreme grief, graphic violence, dead people, nudity or other potentially offensive content require careful consideration before publication. In these cases a photo editor, the assistant managing editor, the managing editor or the editor must be consulted before publication."); *General Privacy Policy*, PASADENA STAR, http://www.pasadenastarnews.com/privacy (last visited Sept. 1, 2009) ("If a question, comment, story, joke, idea or opinion is published, only the student's first name, grade and state/country appear on the site."). Newspapers likely adopted such policies to conform to the Children's Online Privacy Protection Act. *See* 15 U.S.C. §§ 6502–06 (2006).

[140] *See* Dan L. Burk, *The Trouble with Trespass*, 4 J. SMALL & EMERGING BUS. L. 27, 39–54 (2000); Kevin Emerson Collins, *Cybertrespass and Trespass to Documents*, 54 CLEV. ST. L. REV. 41, 41–65 (2006); Jacqueline Lipton, *Mixed Metaphors in Cyberspace: Property in Information and Information Systems*, 35 LOY. U. CHI. L.J. 235, 240–44 (2003).

and may be influenced by courts' broad interpretation of section 230, which grants Web sites immunity from liability for the conduct of their users. Yet section 230 immunity should not be interpreted to mean that Web sites should have no liability whatsoever for the businesses they create.[141]

Arguments disclaiming Web site sponsor responsibility reflect a one-sided and rather socially irresponsible notion of the role of Web site sponsors. Significantly, this view is at odds with expectations of offline business owners. This Part makes two different arguments for why Web site sponsors should adopt the proposals set forth in the preceding section. Both arguments appeal to Web site sponsors' self-interest. The first argument, which is more carrot than stick, posits that greater accountability enhances a Web site sponsor's ability to control its business and image. The second argument, which is more stick than carrot, contends that Web site sponsors should have, and may already have, liability under tort law to address online harassment on their Web sites.

A. Encouraging Self-Regulation

Web site sponsors often express reluctance to regulate communication among users for various reasons, including that such regulation undermines the nature of their Web sites.[142] Many Web sites already have policies in place that mirror some or most of the proposals set forth in Part IV.[143] The primary problem has been in

---

[141] *See* Kim, *supra* note 21, at 116 ("The immunity that website sponsors . . . have as *publishers* should not mean that they have no obligation whatsoever for the activity on their website.").

[142] *See supra* note 9 and accompanying text.

[143] *See* craigslist, *Terms of Use*, http://www.craigslist.org/about/terms.of.use (last visited Sept. 1, 2009) ("You acknowledge that craigslist does not pre-screen or approve Content, but that craigslist shall have the right (but not the obligation) in its sole discretion to refuse, delete or move any Content that is available via the Service, for violating the letter or spirit of the TOU or for any other reason."); MySpace, *Terms of Use Agreement*, http://www.myspace.com/index.cfm?fuseaction=misc.terms (last visited Sept. 1, 2009) ("MySpace may reject, refuse to post or delete any Content for any or no reason, including Content that in the sole judgment of MySpace violates this Agreement or which may be offensive, illegal or violate the rights of any person or entity, or harm or threaten the safety of any person or entity. MySpace assumes no responsibility for monitoring the MySpace Services for inappropriate Content or conduct. If at any time MySpace chooses, in its sole discretion, to monitor the MySpace Services, MySpace nonetheless assumes no responsibility for the Content, no obligation to modify or remove any inappropriate Content, and no responsibility for the conduct of the User submitting any such Content."); eBay, *User Agreement*, http://m.ebay.com/Pages/UserAgreement/US.aspx (last visited Sept. 1, 2009) ("Without limiting other remedies, [eBay] may limit, suspend or terminate our service and user accounts, prohibit access to our website, delay or remove hosted content, and take technical and legal steps to keep users off the sites if we think that they are creating problems, possible legal liabilities, or acting inconsistently with the letter or spirit of our policies. We also reserve the right to cancel unconfirmed accounts or accounts that have been inactive for a long time.").

the reluctance of some Web site sponsors to enforce their own policies. Even Web sites whose very business models appear to encourage harassing behavior have policies prohibiting online harassment.[144]

Brian Leiter, a law professor and well-known blogger, recently explained the rationale underlying his selective open comments policy:

> First, there are likely to be far more anonymous comments, and anonymity generally encourages irresponsible behavior. . . . Second, there would be a lot more spam. . . . Third, the quality of the threads is likely to be much more uneven. . . . I'd rather not have a site bearing my name be the repository for the kind of garbage that is typical on the blogs that do not moderate comments.

A Word on My Comments Policy, BRIAN LEITER'S LAW SCHOOL REPORTS, http://leiterlawschool.typepad.com/leiter/2008/10/a-word-on-my-co.html (Oct. 20, 2008, 3:03). Another law professor and popular blogger has recently abolished the comments section altogether due to trolls and incivility. *See* Jack Balkin, *New Comments Policy at Balkinization*, BALKINIZATION, http://balkin.blogspot.com/2009/01/new-comments-policy-at-balkinization.html (Jan. 29, 2009, 0:17). A law blog recently changed its default comments section to "hidden." *See* David Lat & Elie Mystal, *New Above the Law Comment Policy*, ABOVE THE LAW, http://abovethelaw.com/2009/01/atl_new_comment_policy.php (Jan. 26, 2009, 18:01). Entirely shutting down comments may simply reinforce the idea that the trolls have prevailed, however, and should be carefully considered. Establishing and reinforcing a cultural norm of respect on a particular blog, and changing norms of civility on blogs in general, may result in loosening restrictions on comments policies.

[144] For example, the terms and conditions of Juicy Campus, a Web site that encouraged and disseminated college campus gossip with a promise of anonymity, formerly stated that users agreed not to post content that is "unlawful, threatening, abusive, tortious, defamatory, obscene, libelous, or invasive of another's privacy." *See* Eugene Volokh, *Juicy Campus Lawyer Responds About the New Jersey Attorney General's Investigation*, http://www.volokh.com/posts/1207884421.shtml (Apr. 10, 2008, 23:27). After the Web site was investigated for consumer fraud by the New Jersey attorney general for failing to enforce its own terms and conditions, the Web site changed its terms to expressly disclaim any responsibility for monitoring content:

> You acknowledge that JuicyCampus does not pre-screen Content. You agree that JuicyCampus is under no obligation to review all Content, or any Content, on any regular schedule or at all. You agree that JuicyCampus shall have the right (but not the obligation) to re-arrange, remove and/or restrict access to any Content on the Site at any time in its sole discretion, for any reason or for no reason. BY USING THE SITE, YOU AGREE THAT JUICYCAMPUS SHALL HAVE NO OBLIGATION TO MONITOR CONTENT ON THE SITE OR TO DELETE CONTENT FROM THE SITE, EVEN IF JUICYCAMPUS IS NOTIFIED THAT SUCH CONTENT VIOLATES THIS AGREEMENT. . . . User Conduct Guidelines. JUICYCAMPUS RESERVES THE RIGHT, BUT DISCLAIMS ANY OBLIGATION OR RESPONSIBILITY, TO REMOVE ANY CONTENT THAT DOES NOT ADHERE TO THESE GUIDELINES, IN ITS SOLE DISCRETION.

Web site sponsors may refrain from enforcing their policies because they fear user dissatisfaction with content regulation. The founder of AutoAdmit, who controlled the message board, reportedly feared that removing posts would prompt a mass exodus from his Web site, yet he admitted that his failure to do so meant he "lost his website" to "parasites" and "freaks."[145] The prevailing ethos of the Web is a libertarian one.[146] Any attempt to restrict speech or activity tends to be greeted with cries of censorship, even though the entity seeking to regulate the conduct or the speech is a private actor.[147] For example, a recent video of former Alaska governor and vice presidential candidate Sarah Palin's former church, the Wasila Assembly of God, was removed from YouTube for "inappropriate content."[148] Internet users condemned YouTube's actions as "censorship," comparing the site's decision with government censorship in China and advocating retaliatory measures against YouTube. [149] Speech regulation by private entities, however, is not an infringement of free speech.[150] The First Amendment prohibits the government, not private actors, from restricting speech.[151] Yet many Web site users have grown

---

Juicy Campus, Terms and Conditions, http://www.juicycampus.com/posts/terms-condition (last visited Feb. 2, 2009). JuicyCampus.com shut down February 5, 2009, claiming "growth outpaced [its] ability to muster the resources needed to survive the economic downturn and the current level of revenue generated is simply not sufficient to keep the site alive." Official JuicyCampus Blog, *A Juicy Shutdown*, http://juicycampus.blogspot.com (Aug. 6, 2009, 11:47).

[145] Margolick, *supra* note 2 (noting that even his "timid, belated attempts to weed out the worst abuses . . . prompted open rebellion").

[146] *See* SOLOVE, *supra* note 74, at 110–11 (discussing how the libertarian view "reflects deeply rooted norms that developed among Internet users in the early days of the technology. At that time, the prevailing view was that the Internet was a free zone, and the law should keep out").

[147] *See, e.g.*, Nicole Belle, *YouTube Removes Viral Video on Palin's Churches for Inappropriate Content*, CROOKS AND LIARS, http://crooksandliars.com/2008/09/15/youtube-removes-viral-video-on-palins-churches-for-inappropriate-content (Sept. 14, 2008, 18:00); Daily Kos, *YouTube Censors Viral Video on Palin's Churches*, http://www.dailykos.com/story/2008/9/13/81221/8939/814/597200 (Sept. 13, 2008, 12:33 PDT) (arguing that "YouTube has censored a video documentary that appeared to be close to having an effect on a hard fought and contentious American presidential election").

[148] *See supra* note 147.

[149] *See supra* note 147.

[150] *See* ERWIN CHEMERINSKY, CONSTITUTIONAL LAW: PRINCIPLES AND POLICIES 507 (3d ed. 2006) (noting that "[t]he Constitution's protections of individual liberties and its requirement for equal protection apply only to the government"). In some situations, the Constitution may apply to private actions, such as where the government has enacted laws requiring it. *Id.* at 509–10. There are also limited exceptions to the state action doctrine, notably the "public function" doctrine and the "entanglement exception." *Id.* at 517. Neither of these limited exceptions appears to apply to a general discussion of Web sites.

[151] The First Amendment states that "Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom

accustomed to thinking of the whole of the Internet as a public forum, rather than as privatized Web sites, and many view attempts to restrict activity as censorship.[152]

Web site sponsors are in the best position to regulate communication on their Web sites given concerns about governmental restrictions of speech.[153] While it is popularly assumed that everyone is entitled to communicate on the Internet, everyone is not entitled to communicate everywhere. While the public/private distinction regarding speech has been firmly established in the physical world, there has been a shift in the attitude toward Internet communication, with many arguing that placing restrictions on postings to nongovernmental Web sites amounts to suppression of free speech by Web site sponsors.[154] For example, AutoAdmit defended its controversial message board by saying it was simply a forum for free speech "where people can express themselves freely, just as if they were to go to a town square and say whatever brilliant or foolish thoughts they have."[155] This argument promotes a view that subjects Internet communication to different standards and rules than those that govern offline communication, where private actors are at liberty to regulate speech and conduct on their premises. This Article strongly rejects this sly political stance equating speech regulation on nongovernmental Web sites to censorship.[156] As private actors, Web site sponsors

---

of speech, or of the press; or the right of the people peaceably to assemble, and to petition the Government for a redress of grievances." U.S. CONST. amend. I.

[152] This may be due, in large part, to the absence of public forum for communication. *See* Nunziato, *supra* note 18, at 1117.

[153] This is not to say that government regulation of content on the Internet would necessarily run afoul of the First Amendment. *See* Andrew Chin, *Making the World Wide Web Safe for Democracy: A Medium-Specific First Amendment Analysis*, 19 HASTINGS COMM. & ENT. L.J. 309, 313 (1997) (explaining how "the structural impact of the World Wide Web . . . on the distribution of power in public discourse may justify intervention by the state").

[154] *See* Branscomb, *supra* note 20, at 1641 (noting that "netizens" "assert what they call a First Amendment right of unencumbered access to whatever information they deem personally useful or desirable" and that, although it is "not accurate to describe this claim as a First Amendment right, clearly many Internet users' developing expectation of freely flowing channels of information without censorship by outsiders cannot be ignored").

[155] Nakashima, *supra* note 2, at A1.

[156] This is not to suggest that government censorship of the Internet is not a concern, only that it is not a concern when Web site sponsors themselves regulate the content. It is less of a concern in the United States than it is in other countries. Foreign government censorship of Web content has been the subject of recent news attention. *See* Thomas Crampton, *World Business Briefing Europe: Turkey: YouTube Blocked Over Content Found Offensive*, N.Y. TIMES, Mar. 8, 2007, at C1 (reporting that a court in Turkey ordered blockage of all access to YouTube after a video appeared on the Web site that was deemed insulting to Mustafa Kemal Ataturk, the founder of modern Turkey); Jane Spencer & Kevin J. Delaney, *YouTube Unplugged: As Foreign Governments Block Sensitive Content, Video Site Must Pick Between Bending to Censorship, Doing Business*, WALL ST. J., Mar. 21, 2008, at B1 (discussing China and Turkey's ban on access to YouTube). China banned

have greater freedom to shape social interactions on the Internet and to encourage behaviors that reflect prevailing physical-world social norms. To avoid this responsibility and to ignore that Internet norms are now being created is to default, *Lord of the Flies*-style,[157] to the standards of conduct set by the trolls of the Internet.[158]

The misperception regarding the private nature of Web sites may be partly responsible for the "anything goes" culture that prevails on some Web sites on the part of some users. Because some users regard the ability to post and participate on a Web site as a right, rather than a privilege, they may engage in conduct that ultimately damages the reputation and image of the Web site. MySpace, for example, received much negative public attention from a cyberdeception incident that resulted in the suicide of a teenage girl.[159] YouTube, eBay, and craigslist regularly fend off infringement claims arising from illicit content uploaded by users.[160] Facebook struggles with trolls who misuse information posted on members' pages.[161]

Elevating expectations of Web site sponsor accountability adjusts user expectations of who controls Web site activity and content, and enhances the Web site sponsor's ability to control its image and brand. The guidelines and standards

---

access to YouTube after video clips showing Tibetan monks being dragged through the streets by Chinese soldiers appeared on the site. *Id.*

[157] As Danielle Citron observes, "[i]f we believe that the Internet is, and should remain, a Wild West with incivility and brutality as the norm, then those who are impervious to such conduct will remain online while the vulnerable may not. To that end, we may get more bull-headed, impervious posters and fewer thoughtful ones." Citron, *supra* note 12, at 105.

[158] *See* Schwartz, *supra* note 39, at 26 (defining a cyberspace "troll" as one who "intentionally disrupts online communities").

[159] *See* Susan Duclos, *Indictment Handed Down in MySpace Hoax That Caused Child to Commit Suicide*, DIGITAL J., May 16, 2008, http://www.digitaljournal.com/article/254805 (noting how "information obtained over the MySpace computer system [was used] to torment, harass, humiliate, and embarrass the juvenile MySpace member").

[160] *See* Chi. Lawyers' Comm'n for Civil Rights Under Law, Inc. v. Craigslist, Inc., 519 F.3d 666, 668 (7th Cir. 2008) (lawsuit claiming that craigslist allowed listings that violated the federal Fair Housing Act); Katie Hafner, *Seeing Fakes, Angry Traders Confront EBay*, N.Y. TIMES, Jan. 29, 2006, at 1; Greg Sandoval, *YouTube Sued over Copyright Infringement*, ZDNET NEWS, July 19, 2006, http://news.zdnet.com/2100-9588_22-148863.html.

[161] Facebook's policies expressly state that Facebook has no responsibility for misuse of user content by other users. *See* Facebook Privacy Policy, *Facebook Principles*, http://www.facebook.com/policy.php (last visited Sept. 1, 2009) ("You post User Content (as defined in the Facebook Terms of Use) on the Site at your own risk. Although we allow you to set privacy options that limit access to your pages, please be aware that no security measures are perfect or impenetrable. We cannot control the actions of other Users with whom you may choose to share your pages and information. Therefore, we cannot and do not guarantee that User Content you post on the Site will not be viewed by unauthorized persons.").

established by Web sites in their user agreements and policies might then be taken more seriously by users as contractual requirements. For example, regardless of whether she read MySpace's terms of use, Lori Drew knew that posing as a sixteen-year-old boy to deceive and manipulate another MySpace user was against the company's policies, yet she did so.[162] An extensive user policy prohibits eBay members from selling items that violate third-party rights.[163] Although eBay may have instituted this policy to minimize its legal liability, its policy also ensures that it is viewed as a legitimate and reputable business. YouTube has a policy forbidding graphic violence, sexually explicit images, and "bad stuff like animal abuse, drug abuse, under-age drinking and smoking, or bomb making."[164] This policy helps set user expectations of what is permissible on the site and also of when YouTube will remove site content.[165] By explaining its policies and managing expectations upfront, YouTube is better able to protect its image and brand.

Web site image and branding, in turn, affect mainstream acceptability and corporate sponsorship. For example, rather than being known as a site for porn video clips, YouTube is known for quirky and humorous clips on a wide range of topics, making it a more suitable site for advertisers. Juicy Campus went out of business in February 2009 due to a lack of advertising revenue.[166] Whether the lack of advertising revenue was due to the negative publicity surrounding the Web site and an investigation by the New Jersey attorney general on consumer fraud charges, or simply the result of the economic downturn, was the subject of much speculation.[167]

Marketed in the right way, some anti-cyberharassment measures may be viewed as features or Web site advantages. While some users may resist any imposition of restraints, others may appreciate their potential for deterring impulsive behavior. For example, Google recently introduced an optional Gmail feature called "Mail Goggles," which incorporates contractual restraints to prevent embarrassing user behavior. [168] The feature prompts a user with a pop-up window

---

[162] *See* Nancy S. Kim, *Playing by the Rules of the Cyber Playground*, THE PROVIDENCE J., July 4, 2008, *available at* http://www.projo.com/opinion/contributors/content/CT_kim4_07-04-08_FDAN168_v20.411deb6.html (last visited Sept. 1, 2009).

[163] EBay, *Your User Agreement*, http://pages.ebay.com/help/policies/user-agreement.html (last visited Sept. 1, 2009).

[164] YouTube, *YouTube Community Guidelines*, http://www.youtube.com/t/community_guidelines (last visited Sept. 1, 2009).

[165] *See id.*

[166] *See* Matt Ivester, *A Juicy Shutdown*, http://juicycampus.blogspot.com (Feb. 4, 2009, 11:47 PST).

[167] *See* Jason Kincaid, *JuicyCampus Dries Up*, TECH CRUNCH, Feb. 4, 2009, http://www.techcrunch.com/2009/02/04/juicycampus-dries-up; Cara Sprunk, *Cornell University Reacts to Juicy Campus Closure*, CORNELL SUN, Feb. 6, 2009, http://cornellsun.com/section/news/content/2009/02/06/cu-reacts-juicy-campus-closure.

[168] Jon Perlow, *New in Labs: Stop Sending Mail You Later Regret*, http://gmailblog.blogspot.com/search?q=Jon+Perlow (Oct. 6, 2008, 18:25 PDT).

that asks, "Are you sure you want to send this?" if the user tries to send e-mail during certain times when the user is more likely to be inebriated (i.e., late night to early morning).[169] Users are then required to solve several math problems before Google will permit the message to be sent.[170]

Web site sponsors should voluntarily adopt online harassment policies before Congress mandates them.[171] In the aftermath of the MySpace case, legislators have proposed laws that would criminalize cyberharassment,[172] although some fear that some of the proposed laws are overbroad.[173] Several commentators have suggested that section 230 of the CDA should be amended so Web site sponsors receive a type of limited immunity based upon lack of actual notice, rather than absolute immunity.[174] Others, however, have noted that a notice-and-takedown scheme may put Web site sponsors in the awkward position of having to make legal determinations of what constitutes defamatory or otherwise tortious material.[175] Although the focus of this Article is on private law approaches to online harassment, it is worth noting that the success of any such approaches may have the effect of curbing government regulation.

My suggested anti-cyberharassment proposals are intended to deter impulsive, regrettable behavior by forcing posters to think before pressing "send." The effect may be to evaluate and filter speech, but it is the poster, not a government actor, who is censoring communication. The proposals provide an opportunity for contemplation without imposing a ban on speech, leaving the decision whether to

---

[169] *Id.*

[170] *Id.*

[171] Congress should also revisit section 230 of the Communications Decency Act to determine whether the definition of "interactive computer service" should be limited to Internet service providers and not Web site sponsors, and/or whether to qualify immunity. An interactive computer service is defined as "any information service, system, or access software provider that provides or enables computer access by multiple users to a computer server, including specifically a service or system that provides access to the Internet and such systems operated or services operated by libraries or educational institutions." 47 U.S.C. § 230 (2006).

[172] Stefanie Olsen, *A Rallying Cry Against Cyberbullying*, http://news.cnet.com/8301-10784_3-9962375-7.html?part=rss&subj=news&tag=2547-1_3-0-20 (June 7, 2008, 6:00 PDT).

[173] Mark "Rizzn" Hopkins, *Should There be a Law Against Asshats Like Me?*, http://mashable.com/2008/06/09/asshats/ (June 9, 2008) (fearing that pending legislation will have the effect of criminalizing posts criticizing celebrities and mainstream media).

[174] *See* SOLOVE, *supra* note 74, at 154 (arguing that once a Web site is notified about a cyberharassment problem, it should respond to the problem or be liable); *see also* Bradley A. Areheart, *Regulating Cyberbullies Through Notice-Based Liability*, 117 YALE L.J. POCKET PART 41, 43 (2007), *available at* http://thepocketpart.org/2007/09/08/areheart.html (arguing for ISP liability based upon a notice and takedown scheme based on actual notice).

[175] *See* Citron, *supra* note 12, at 122; Lemley, *infra* note 182, at 801–02 (noting the problems with the copyright notice and takedown regime and proposing one based upon the trademark immunity statute).

post the communication in the hands of the poster. The government could arguably adopt even more onerous content-neutral restrictions without violating free speech principles.[176] The government has chosen not to regulate the Internet, but that does not mean that if it were to do so its actions would be unconstitutional.[177]

Although many Web sites work to minimize online harassment, some Web sites actively encourage it.[178] Rather than seeking a more commercially acceptable image, these Web sites craft an alternative niche for themselves as a place where users can malign others.[179] Although carrot-like incentives may work for those Web sites striving for mass market acceptance , some Web sites may need a more stick-like measure.

B. Imposing Proprietorship Liability on Web Site Sponsors

One stick-like measure may be the imposition of tort liability on Web site sponsors. In a prior essay, I argued that proprietorship liability should be imposed upon Web site sponsors.[180] I analogized the duty of Web site sponsors to brick-and-mortar businesses and advocated the imposition of liability similar to the "premises" liability imposed on offline businesses. The analogy to premises liability is not a perfect one given the differences between the Internet and the physical world, including the inability to draw secure boundaries and screen for potential harm. Nevertheless, the important similarity is that offline and online business owners establish, control, and benefit from their businesses. Web site sponsors are proprietors who exercise control over their businesses in many ways. Web site sponsors enforce their proprietorship over their Web sites by establishing terms of use in clickwrap or browsewrap agreements. Web sites may capitalize on their proprietorship by selling user information to advertisers. They may sell advertising space or products, such as T-shirts, directly on their Web sites. They may receive a percentage of revenues that their users receive from the sale of products on their Web sites. They may also profit indirectly by using their Web sites as marketing platforms to reach a broad audience. They may then sell

---

[176] One such proposal is the Internet Community Ports Act, which would entail assigning ranges of "ports" or channels for information transmission to different purposes. *See* Cheryl B. Preston, *Making Family-Friendly Internet a Reality: The Internet Community Ports Act*, 2007 BYU L. REV. 1471, 1475–78; Cheryl B. Preston, *Zoning the Internet: A New Approach to Protecting Children Online*, 2007 BYU L. REV. 1417, 1468–69.

[177] *See* Tushnet, *supra* note 15, at 988 (arguing that "Congress is free, within rather broad limits, to determine an appropriate intermediary liability regime").

[178] *See supra* note 9 and accompanying text.

[179] *See supra* note 9 and accompanying text. For additional examples of such Web sites, see DontDateHimGirl.com, http://www.don'tdatehimgirl.com (last visited Sept. 1, 2009); GossipReport.com, http://www.gossipreport.com (last visited Sept. 1, 2009); EncyclopediaDramatica.com, http://www.encyclopediadramatica.com (last visited Sept. 1, 2009).

[180] Kim, *supra* note 21, at 116.

ancillary products or services, such as books or consulting services, to this audience.

Although some scholars and commentators argue that Web sites are property and should be treated as such, others disagree.[181] Even those who disagree that Web sites are "just like" property must recognize that Web site sponsors maintain control over the content of the site (regardless of whether they choose to exercise that control) and are in the best position to prevent harm to other users on the site. Of course, any discussion of Web site sponsor liability must recognize the difficulties inherent in applying laws and norms developed with the physical world in mind to cyberspace, and proposed remedies must address those difficulties. Yet many of the criticisms of the Web-site-as-property view pertain to the difficulties of delineating boundaries of intangible works.[182] These concerns are inapposite where the activity at issue is limited to what happens on the Web site.

---

[181] This Article bypasses the complex issue of whether Web site ownership and intellectual property generally are akin to tangible property ownership for fear of distracting from the Article's central issues. The topic has been discussed at length elsewhere. *See* Frank H. Easterbrook, *Intellectual Property is Still Property*, 13 HARV. J.L. & PUB. POL'Y 108, 111 (1990); I. Trotter Hardy, *Not So Different: Tangible, Intangible, Digital, and Analog Works and Their Comparison for Copyright Purposes*, 26 U. DAYTON L. REV. 211, 213 (2001) (asserting that "[t]hese assumptions of differences [between intangible intellectual property and tangible property] are wrong"); I. Trotter Hardy, *Property (and Copyright) in Cyberspace*, 1996 U. CHI. LEGAL F. 217, 246 (1996) (arguing that "it seems no harder to identify an informational work in cyberspace as a unit with "boundary lines" than it is to identify a similar informational work elsewhere"); Jacqueline Lipton, *Mixed Metaphors in Cyberspace: Property in Information and Information Systems*, 35 LOY. U. CHI. L.J. 235, 240–244 (2003) (critiquing the use of property metaphors in cyberspace); Michael J. Madison, *Rights of Access and the Shape of the Internet*, 44 B.C. L. REV. 433, 464–71 (2003) (explaining why trespass to intangibles is significantly different from trespass to chattels). *But see* Burk, *supra* note 140, at 28 (noting that proprietary interest in the Internet has "only the most tenuous of antecedents in the law of chattels"); Mark A. Lemley, *Property, Intellectual Property, and Free Riding*, 83 TEX. L. REV. 1031, 1032 (2004) (contending that "full internalization of positive externalities is not a proper goal of tangible property rights except in unusual circumstances"). There is a split of case authority on whether to treat Web sites and computer servers as "chattels." *See* eBay Inc. v. Bidder's Edge., Inc., 100 F. Supp. 2d 1058, 1073 (N.D. Cal. 2000) (holding that eBay's servers were private property and finding that unauthorized access was a trespass); Register.com, Inc. v. Verio, Inc., 126 F. Supp. 2d 238, 248–51 (S.D.N.Y. 2000) (holding that an automated software robot searching a database without permission constituted a trespass to chattels). *Contra* Intel Corp. v. Hamidi, 71 P.3d 296, 311 (Cal. 2003) (holding that the tort of trespass to chattels did not encompass electronic communication that did not damage or impair the computer system).

[182] *See* Brett Frishmann & Mark A. Lemley, *Spillovers*, 107 COLUM. L. REV. 257, 274 (2007) (noting the difficulty in determining whether a user has "trespassed" because of the lack of defined boundaries); Mark A. Lemley & Philip J. Weiser, *Should Property or Liability Rules Govern Information*, 85 TEX. L. REV. 783, 790 (2007) (noting that property rules may impede the "efficient functioning of the Internet"); Henry E. Smith, *Intellectual*

Sponsors of publicly accessible Web sites are "proprietors," whether the Web site is a blog, a gossip site, or a retail site. Along with ownership comes responsibility. Because the Web sites are publicly accessible (again, this Article is limited to content only on publicly accessible Web sites), they are more akin to businesses than to private residences. Although some sites sell products and are clearly "for profit," other sites are less clearly commercial. Yet even sites that are not obviously retail-oriented have the ability to monetize their content in some way, such as by selling ancillary products like T-shirts, selling advertising or user data, or by using the site as a marketing vehicle to sell products, such as a novel, or services, such as consulting.[183] In some cases, a Web site may intend to generate a large readership in the hopes of eventually selling out to a larger commercial entity. This Article uses the term "proprietorship" or "proprietary interest" to refer to a Web site sponsor's ability to capitalize upon the activity on a Web site, regardless of whether it in fact chooses to do so. It thus avoids the larger question of whether Web sites are the "property" of the Web site sponsor.

Tort law places upon a "possessor of land" or "premises occupier" a duty to exercise reasonable care to avoid foreseeable harm caused by the accidental, negligent, or intentionally harmful acts of third parties.[184] This duty is not to ensure the safety of invitees, but to take "reasonable measures" to control the conduct of third parties, or to give adequate warning to enable invitees to avoid harm.[185] Accordingly, the owner is liable for negligence only where the owner failed to take reasonable care to discover the occurrence of dangerous conduct by third parties, or where the owner failed to exercise reasonable care to provide appropriate precautions. For example, an owner may be found to have failed to exercise

---

Property as Property: Delineating Entitlements in Information, 116 YALE L.J. 1742, 1748–49 (2007).

[183] In some high-profile cases, controversial blogs have succeeded in generating enough publicity to secure a book publishing deal. *See* Lester Haines, *Washington Sex Blogger Signs Book Deal*, THE REGISTER, July 2, 2004, http://www.theregister.co.uk/2004/07/02/blogger_book_deal; Allen Salkin, *Why Blog? Reason No. 92: Book Deal*, N.Y. TIMES, Mar. 30, 2008, at ST1.

[184] The Restatement (Second) of Torts states:

> A possessor of land who holds it open to the public for entry for his business purposes is subject to liability to members of the public while they are upon the land for such a purpose, for physical harm caused by the accidental, negligent, or intentionally harmful acts of third persons or animals, and by the failure of the possessor to exercise reasonable care to (a) discover that such acts are being done or are likely to be done, or (b) give a warning adequate to enable the visitors to avoid the harm, or otherwise to protect them against it.

See RESTATEMENT (SECOND) OF TORTS § 344 (1977).

[185] Murphy v. Penn Fruit Co., 418 A.2d 480, 482 (Pa. Super. Ct. 1980); Exxon Corp. v. Tidwell, 867 S.W. 2d 19, 21 (Tex. 1993) (noting that a landowner has "a duty to protect invitees on the premises from criminal acts of third parties if the landowner knows or has reason to know of an unreasonable risk of harm to the invitee").

reasonable care for failure to provide security personnel or adequate lighting in a parking lot.[186] A California court held that the owners of a restaurant could be found negligent for failing to protect customers where the layout of the restaurant required customers to stand in front of parking spaces with low barriers.[187]

The critical factor in determining whether there was a duty of care (a prerequisite to a finding of negligence) is foreseeability—whether the business owner knew or should have known that the harm was likely to occur on the premises.[188] For example, in one case, a tavern customer verbally threatened the plaintiff and was escorted out of the tavern.[189] The tavern employees then allowed the abusive customer to re-enter the tavern, and the customer attacked the plaintiff.[190] The court found that the tavern had a duty to exercise reasonable care to control the customer's conduct to prevent harm to the plaintiff, and that the duty arose "by reason of the defendant's knowledge that an assault . . . was 'about to occur'" in the tavern.[191]

Two different tests determine foreseeability.[192] The first is the "prior similar incidents" test, under which a duty arises when incidents similar to the harm at issue should have put the business owner on notice.[193] The second test is the "totality of the circumstances" test, whereby the court examines not just whether there were prior similar incidents, but also factors such as whether the business was located in a high-crime area.[194] The Restatement (Second) of Torts also considers the character of the business in determining foreseeability:

> Since the possessor is not an insurer of the visitor's safety, he is ordinarily under no duty to exercise any care until he knows or has reason to know that the acts of the third person are occurring, or are about to occur. He may, however, know or have reason to know, from past experience, that there is a likelihood of conduct on the part of third persons in general which is likely to endanger the safety of the visitor, even though he has no reason to expect it on the part of any particular

---

[186] *See Murphy*, 418 A.2d at 482; *see also* RESTATEMENT (SECOND) TORTS § 344 (1977).

[187] Barker v. Wah Low, 19 Cal. App. 3d 710, 717 (1971).

[188] *But see* Michael J. Yelnosky, *Business Inviters' Duty to Protect Invitees from Criminal Acts*, 134 U. PA. L. REV. 883, 883–84 (1986) (arguing that courts should adopt an unqualified duty-to-protect rule that would require all business inviters to take reasonable steps to prevent crime on their premises).

[189] Gupton v. Quicke, 442 S.E.2d 658, 659 (Va. 1994).

[190] *Id.*

[191] *Id.* at 658; *see also* Bartosh v. Banning, 251 Cal. App. 2d 378, 384 (1967) (holding that one who operates a bar "must act as a reasonable man to avoid harm from the negligence of other persons who have entered the premises or even from intentional attacks on the part of such third persons").

[192] Seibert v. Vic Regnier Builders, Inc., 856 P.2d 1332, 1335–36 (Kan. 1993).

[193] *Id.* at 548–49.

[194] *Id.*

> individual. If the place or character of his business, or his past experience, is such that he should reasonably anticipate careless or criminal conduct on the part of third persons, either generally or at some particular time, he may be under a duty to take precautions against it, and to provide a reasonably sufficient number of servants to afford a reasonable protection.[195]

A duty analogous to possessors of land may be imposed upon Web site sponsors who fail to exercise reasonable care to provide appropriate precautions to prevent or minimize online harassment on their Web sites. This duty would arise where the Web site sponsor has notice of harm or the likelihood of harm to invitees by third parties. The Web site sponsor may have notice either because of similar prior incidents or because the nature of the Web site made such harm foreseeable.

In *Doe v. MySpace*, the court expressly declined to apply premises-based liability to the Internet context.[196] There, the minor plaintiff sued the online social networking site MySpace after she was sexually assaulted.[197] One of the plaintiff's claims contended that MySpace failed to implement basic safety measures to prevent sexual predators from communicating with minors on MySpace.[198] The court rejected the argument, stating the plaintiff cited no precedent for treating a Web site as a virtual premises.[199] Yet the court's opinion reveals it was primarily concerned that the remedy the plaintiff sought would impose an undue burden on MySpace's business:

> Plaintiffs allege MySpace can be liable under a negligence standard when a minor is harmed after wrongfully stating her age, communicating with an adult, and publishing her personal information. To impose a duty under these circumstances for MySpace to confirm or determine the age of each applicant, with liability resulting from negligence in performing or not performing that duty, would of course stop MySpace's business in

---

[195] RESTATEMENT (SECOND) OF TORTS § 344 cmt. f (1977); *see also* Barker v. Wah Low, 97 Cal. Rptr. 85, 88 (1971) (noting that Restatement principles "have been recognized and applied" in California). Some courts have expressly rejected the Restatement view that the character of the defendant's business may be considered in a foreseeability analysis. *See* Timberwalk Apartments, Partners, Inc. v. Cain, 972 S.W.2d 749, 758–59 (Tex. 1998).

[196] *See* Doe v. MySpace, 474 F. Supp. 2d 843, 851 (W.D. Tex. 2007) ("The court declines to extend premises liability cases to the internet context, especially where, as here, the Defendant provides its services to users for free."); *see also* Goddard v. Google, Inc., No. C 08-2738 JF, 2008 WL 5245490, at *4–5 (N.D. Cal. Dec. 17, 2008) (citing to *Doe v. MySpace* to reject characterization of claim as one of receiving "tainted funds" rather than hosting content).

[197] Doe v. MySpace, 528 F.3d 413, 416–17 (5th Cir. 2008).

[198] *Id.* at 416.

[199] *Id.* at 418–20.

> its tracks and close this avenue of communication, which Congress in its wisdom has decided to protect.[200]

In other words, the court appears to base its decision on the reasonableness of MySpace's safety procedures given the vast amount of traffic on its Web site, and the minor's knowing violation of those procedures, instead of explaining why premises-based liability is wholly inapplicable on the Internet.[201] But consider this: if MySpace had no safeguards,[202] and 50 percent of teens using MySpace had been assaulted by sexual predators (even though they accurately stated their age during registration), would the court have reached the same conclusion? Taking the court's statements regarding blanket immunity at face value, MySpace would have no obligation to improve its business model or adopt safety measures to protect further assaults because it was merely the "publisher" of communications between the minor victim and the assailant.[203] Yet such a conclusion would be socially unacceptable.

Given the difference between physical world business premises and Web site premises, the analogy of "possessors of land" to Web site sponsors is limited to just that—an analogy. A theory of liability based upon Web site proprietorship must recognize the differences between Web-based businesses and businesses with physical locations.

Internet-based businesses may have millions of weekly site visitors, compared with brick-and-mortar businesses, which may have dozens; accordingly, the ability to successfully police virtual premises may be more elusive. A determination of what constitutes reasonable proprietorship conduct should take into account the vast amount of Web site traffic. While one attack in an underground parking lot may suffice to put a brick-and-mortar store on notice of the existence of a harmful condition, and thus create an obligation to remedy the condition, one harmful incident of online harassment would not be enough to establish foreseeability on a Web site with thousands of daily postings.

---

[200] *MySpace*, 474 F. Supp. 2d at 851.

[201] The district court merely "decline[d] to extend premises liability cases to the internet context particularly where, as here, the Defendant provides its services to users for free. Plaintiff has cited no case law indicating that the duty of a premises owner should extend to a website as a 'virtual premises.'" *Id.*

[202] MySpace sets the default for users age fourteen and fifteen at "private" rather than "public" so that their profiles are not searchable or viewable by anyone other than their named friends. Joint Statement on Key Principles of Social Networking Sites Safety, http://www.ag.state.mn.us/PDF/PressReleases/SocialNetworkingSitesSafety.pdf (last visited Sept. 1, 2009).

[203] *Myspace*, 474 F. Supp. 2d at 849 ("It is quite obvious the underlying basis of Plaintiffs' claims is that, through posting on MySpace, Pete Solis and Julie Doe met and exchanged personal information which eventually led to an in-person meeting and the sexual assault of Julie Doe. . . . No matter how artfully Plaintiffs seek to plead their claims, the Court views Plaintiffs' claims as directed toward MySpace in its publishing, editorial, and/or screening capabilities.").

Although the cases addressing business owner liability concerned physical harm to invitees, there is nothing in the underlying rationale of these cases that would preclude nonphysical harm. It makes sense to permit recovery for incorporeal injuries that are unique to, and arise from, the incorporeal nature of the business premises. Furthermore, where nonphysical harm, such as defamation, is conducted on physical premises, plaintiffs can sue defendants directly for republication or dissemination of defamatory matter and have no need to rely upon a premises liability theory.[204] But this remedy is unavailable to plaintiffs alleging online harassment because of the immunity granted to Web site sponsors under the Communications Decency Act.

Businesses have also been held liable for their conduct and business activities, not simply their control over premises. For example, business owners have been found liable for injuries caused by third parties during the course of promotional activities. In one case, the defendant planned to drop table tennis balls from an airplane as part of a promotion.[205] Each ball contained a certificate entitling the holder to a prize from the defendant store.[206] The plaintiff went to the site of the promotion and was injured by the crowd that rushed to retrieve the fallen balls.[207] The Supreme Court of Alabama held that "when a proprietor or storekeeper causes a crowd of people to assemble pursuant to a promotional activity, then that person owes a duty to exercise reasonable care commensurate with foreseeable danger or injury to protect those assembled from injuries resulting from the . . . crowd[.]"[208]

A business may be found liable even where the promotional activities occur off-site. For example, a radio station was held liable for the wrongful death caused

---

[204] *See* Hellar v. Bianco, 244 P.2d 757, 759 (Cal. Ct. App. 1952) (holding tavern owner could be held liable for republication of defamatory matter regarding plaintiff by failing to remove such matter from men's room wall after having reasonable opportunity to do so); Fogg v. Boston & L.R. Co., 20 N.E. 109, 109–10 (Mass. 1889) (defendant railroad held liable for posting in office libelous newspaper extract about plaintiff railroad broker for forty days). Describing what constitutes publication, the Restatement (Second) of Torts states:

> (1) Publication of defamatory matter is its communication intentionally or by a negligent act to one other than the person defamed.
>
> (2) One who intentionally and unreasonably fails to remove defamatory matter that he knows to be exhibited on land or chattels in his possession or under his control is subject to liability for its continued publication.

RESTATEMENT (SECOND) OF TORTS § 577 (1977). *But cf.* Scott v. Hull, 259 N.E.2d 160, 161 (Ohio Ct. App. 1970) (finding failure of building owner or agent to remove defamatory graffiti on the outside of building was not grounds for defamation suit because building owner and agent did not engage in "positive acts," such as inviting public into premises).

[205] *See* F.W. Woolworth v. Kirby, 302 So. 2d 67, 68–69 (Ala. 1974).

[206] *Id.* at 68.

[207] *Id.*

[208] *Id.* at 71.

by a radio station listener who was participating in a promotional activity.[209] The radio station conducted a contest that rewarded the first contestant to locate a traveling disc jockey.[210] Two minors, in pursuit of the disc jockey, negligently forced the decedent's car off the highway.[211] In determining whether the defendant radio station owed a duty to the decedent arising out of its broadcast of the giveaway contest, the California Supreme Court noted that a "number of considerations may justify the imposition of duty in particular circumstances, including the guidance of history, our continually refined concepts of morals and justice, the convenience of the rule, and social judgment as to where the loss should fall."[212]

As previously mentioned, Web site sponsors under section 230 are immune from liability for content posted by users on their Web sites.[213] Congress, in passing this legislation, intended to encourage the development of the Internet[214] and to protect "good Samaritan" ISPs from liability for blocking or screening obscene material.[215] Court decisions, however, have applied the immunity

---

[209] *See* Weirum v. RKO Gen., 539 P.2d 36, 45–47 (Cal. 1975).

[210] *Id.* at 37.

[211] *Id.*

[212] *Id.* at 39.

[213] *See supra* notes 13–15 and accompanying text.

[214] *See* Communications Decency Act, 47 U.S.C. § 230(b)(1) (2006) ("It is the policy of the United States: (1) to promote the continued development of the Internet and other interactive computer services and other interactive media.").

[215] *Id.* Section 230 further provides:

> (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 services 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).

Id. The Ninth Circuit recently elaborated that in passing section 230, Congress intended to allow interactive computer services 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. In other words, Congress sought to immunize the *removal* of

provision too broadly.[216] As a consequence, the very section intended to protect Web sites that screen and remove offensive content is now being used as a shield by Web sites to actively encourage the posting of such content.[217] For example, the founder of Juicy Campus, a now-defunct Web site that encouraged its college student users to post gossip, stated on the site blog: "Juicy Campus is the provider of an interactive computer service."[218] He cited section 230 to support his claims that "Juicy Campus is immune from liability from content posted by users."[219] Another Web site encourages users to anonymously post gossip about others, and even suggests they create profiles for other people.[220] The purpose of one Web site is specifically to provide a forum where women can post negative information about the men they have dated.[221] Other Web sites encourage users to post sexually graphic videos and photographs of their ex-lovers.

The imposition of proprietorship liability on Web site sponsors furthers the legislative intent of section 230. The intent underlying section 230 immunity, at least as interpreted by courts, is to both permit Web site sponsors to monitor content and relieve them of the burden of doing so.[222] This intent is understandable given that, at least on some Web sites, the amount of content would make screening and filtering an onerous responsibility.[223] The imposition of

---

user-generated content, not the *creation* of content . . . ." Fair Housing Council of San Fernando Valley v. Roommates.com, LLC, 521 F.3d 1157, 1163 (9th Cir. 2008).

[216] *See, e.g.*, Zeran v. America Online, Inc., 129 F.3d 327, 332 (4th Cir. 1997) (holding that the Communications Decency Act immunized interactive computer service provider that hosted message board, even though it refused to remove false statement after notice); *see also* Lyrissa Barnett Lidsky, *Silencing John Doe: Defamation and Discourse in Cyberspace*, 49 DUKE L.J. 855, 871–82 (2000) ("[C]ourt decisions interpreting subsection 230(c) have broadened its ambit far beyond merely protecting 'Good Samaritan' editorial control. As interpreted, section 230 gives ISPs complete immunity from liability for defamatory content initiated by third parties, even if the ISP consciously decides to republish the defamatory content. The practical effect of these interpretations of section 230 of the CDA is to leave Internet defamation victims with no deep pocket to sue. The defamed plaintiff can no longer sue the intermediary who republished a defamatory communication. Instead, the plaintiff must go to the source and sue the person who originated the defamatory communication, even if that person is an unknown John Doe.").

[217] *See supra* notes 13–15 and accompanying text.

[218] Matt Ivester, *Hate Isn't Juicy. A Letter from the Founder of JuicyCampus.com*, http://juicycampus.blogspot.com/2008/02/hate-isnt-juicy-letter-from-founder-of.html (Feb. 29, 2008, 15:59 PDT).

[219] *Id.*

[220] *See* GossipReport.com, http://www.gossipreport.com/ (last visited Sept. 1, 2009) ("On GossipReport.com you can anonymously talk about anyone you want. Instead of creating a profile about yourself, you can create a profile about someone else. Get in the loop. Go Gossip!").

[221] DontDateHimGirl.com, http://dontdatehimgirl.com/home/ (last visited Sept. 1, 2009).

[222] *See supra* notes 13–15 and accompanying text.

[223] *See* Brief of Defendant-Appellee at 4, Chi. Lawyers' Comm'n for Civil Rights Under Law, Inc. v. Craigslist, Inc., 519 F.3d 666 (7th Cir. Dec. 4, 2007) (No. 07-1101)

proprietorship-based tort liability would not mean an obligation to screen or filter content, as the Web site sponsor would not be liable for information posted by third parties. Nor would it require Web site sponsors to determine whether a particular post is defamatory or otherwise criminal or tortious. While it may not be reasonable to expect a Web site sponsor to filter numerous messages prior to posting, it is reasonable to expect it to establish and enforce policies to discourage online harassment. The standard for liability would be negligence based upon the nature of the business (including volume of traffic), not strict liability. Negligence on the part of the Web site sponsor then would mean that it failed to take reasonable steps to *prevent or deter* foreseeable online harassment.

The determination of reasonableness and foreseeability should consider the nature of the Web site, including the number of daily visitors and the size of the business. A leanly staffed business such as craigslist,[224] for example, which receives millions of weekly visitors,[225] should not be expected to prescreen or to make content-based decisions regarding user postings. Web sites like Dontdatehimgirl.com (whose motto is "don't date him until you check him out first"[226]) or EncyclopediaDramatica (whose motto is "in lulz we trust"),[227] on the other hand, that actively encourage users to anonymously and impulsively (i.e., without a cooling period or registration requirement) post inflammatory material about private individuals, are merely exploiting their section 230 immunity.

Given Congress's objectives in implementing section 230 and the vast amount of traffic on many Web sites, Web site sponsors generally should not be required to implement procedures to prescreen or make subjective determinations of the lawfulness of user-supplied content. A Web site sponsor, however, should be liable for the harm that results from its negligence in setting up its Web site and for a business model that fails to incorporate reasonable steps or safeguards to prevent or minimize foreseeable harassment.

To establish reasonable conduct, Web site sponsors should adopt anti-cyberharassment policies and procedures, such as those set forth in Part IV, to prevent or reduce the likelihood of online harassment. A complete absence of such policies or a business model that encourages harassing behavior would indicate a breach of this duty. Similarly, a failure to enforce anti-cyberharassment policies might indicate negligence.

(giving examples that the popular online classified advertising Web site craigslist reportedly received more than ten million new notices in a typical month in 2006).

[224] Cragislist, http://www.craigslist.org/about/factsheet (last visited Sept. 1, 2009) (stating that craigslist has thirty employees).

[225] *Id.* (stating that craigslist receives more than twenty billion page views each month, and that fifty million people (including forty million in the United States) use the Web site's services each month).

[226] DontDateHimGirl.com, http://dontdatehimgirl.com/home/ (last visited Sept. 1, 2009).

[227] Encyclopedia Dramatica, http://www.encyclopediadramatica.com/Main_Page (last visited Sept. 1, 2009).

In addition, a Web site should be liable for its conduct in responding to harassment complaints. For example, one of the female law students in the AutoAdmit case e-mailed one of the Web site's founders and requested that he take down certain offensive posts about her.[228] He responded in an AutoAdmit post and warned that if he kept receiving similar requests, he would post them on the message board.[229] While not liable for the content of users' posts, AutoAdmit should be liable for its own conduct and for responding to the takedown request in an unreasonable manner (i.e., through intimidation and public humiliation). Another Web site reputedly[230] asks requestors to submit a fee before considering any takedown request.[231] In addition, the appeal process is allegedly a sham, and the requesting party's pleas for mercy are uploaded onto the Web site for further ridicule and "lulz."[232] The plaintiff would have to establish harm before charging that the Web site sponsor's negligence was responsible for the harm; however, it would be the Web site's own actions for which it would be liable. The possibility of being subject to tort liability may prod Web site sponsors who are otherwise unwilling to self-regulate into adopting policies and procedures to reduce or eliminate online harassment.

C. Imposing Proprietorship Liability Conforms to Objectives of Tort Law

The call for greater Web site sponsor accountability is a call for a normative shift in the way we view online harassment. Requiring a certain level of accountability on the part of Web site sponsors is not particularly shocking. They are currently held accountable to a certain extent for copyrighted materials on their site.[233] Web site sponsors adopt a hypocritical position by claiming their Web sites are public forums and that they are constrained by free speech concerns from taking any action to prevent online harassment, while at the same time treating their Web sites as "private property" for commercial gain by, for example, selling

---

[228] Margolick, *supra* note 2.

[229] *Id.*

[230] The author received an anonymous letter from a victim of the Web site regarding the takedown appeal process at this particular Web site. The author was unable to confirm the takedown appeal process at this particular Web site without submitting a fee and undergoing it herself, which she for obvious reasons was unwilling to do.

[231] *Id.*

[232] "Lulz" is the term used to describe laughing at another's expense. Mattathias Schwartz, *The Trolls Among Us*, N.Y. TIMES, Aug. 3, 2008, at MM24 (defining "lulz" as "[a] corruption of 'LOL' or 'laugh out loud,' 'lulz' means the joy of disrupting another's emotional equilibrium").

[233] Web sites may take down material if they are served with a takedown notice under the Digital Millennium Copyright Act ("DMCA") that the material is infringing rather than waiting for a court to definitively make such a decision. *See* Vernor v. Autodesk, Inc., 555 F. Supp. 2d 1164, 1165 (W.D. Wash. 2008) (plaintiff sued Autodesk because it sent an infringement notice to eBay, where the plaintiff was selling copies of Autodesk software products, and eBay suspended the auction in response to the notice and eventually suspended the plaintiff's eBay account without waiting for a court to resolve the matter).

advertising. Of course Web site sponsors are at liberty to cater to users' preferences and desires, but in doing so they should be held liable for users' abuses. The business models of certain Web sites are specifically intended to encourage behavior that is likely to result in online harassment.[234] One Web site encourages posters to submit gossip and states not only that all posts are anonymous but that users can create profiles of *other* individuals and post using those profiles.[235] It encourages posters to submit "pics and videos to really tell the story!"[236] These Web sites should be viewed as having made a calculated business decision to permit "high risk" activity on their Web sites, and their liability should reflect that calculation. Web site sponsors that encourage harmful behavior, even if they do so slyly, should be held accountable for the ill effects resulting from their business models. On the other hand, Web site sponsors that have implemented policies to deal with online harassment and that enforce such policies should not be held liable for the conduct of their users.

The imposition of proprietorship liability upon Web site sponsors furthers the objectives of tort law.[237] It deters antisocial conduct and compensates those injured by such conduct.[238] It allocates the risk of injury to the party in the best position to avoid its occurrence and absorb the loss.[239] The burden on the Web site sponsor in adopting an online harassment policy is less than the likelihood of injury from failure to adopt such a policy, especially given that the duty does not arise unless the injury was foreseeable.[240]

Some critics may argue that my proposed model of liability lacks defined parameters and will make it difficult for Web site sponsors to ascertain what steps they must take to avoid liability. As a result, the argument goes, innovation may suffer as businesses decline to pursue new ventures for fear of being sued. But entrepreneurship has never come with guarantees, and imposing tort liability upon Web site sponsors is no different from tort liability imposed upon offline

---

[234] For example, Juicy Campus's slogan was "C'mon. Give us the juice. Posts are totally 100 percent anonymous." *See* Alexandria Phillips, *College Web Page Spreads Rumors*, THE TRIANGLE.ORG, Jan. 16, 2009, http://media.www.thetriangle.org/ (in search box, enter title of article). The New York Times described Juicy Campus as "a dorm bathroom wall writ large, one that anyone with Internet access can read from and post to." Richard Morgan, *A Crash Course in Online Gossip*, N.Y. TIMES, Mar. 16, 2008, at ST 7.

[235] *See supra* note 220.

[236] *Id.*

[237] *See* Doug Licthman & Eric Posner, *Holding Internet Service Providers Accountable*, 12 SUP. CT. ECON. REV. 221, 221–28 (2006) (arguing that immunity for intermediaries is difficult to defend on policy grounds and is inconsistent with conventional tort law principles).

[238] John C.P. Goldberg, *Twentieth Century Tort Theory*, 91 GEO. L.J. 513, 524–26 (2003).

[239] Lawrence v. Bainbridge Apartments, 957 S.W.2d 400, 405 (Mo. Ct. App. 1997) (noting the objective of tort law is to place the cost of the injury on the party in the best position to avoid the risk and absorb the loss).

[240] This is an articulation of the formula, B<PL, famously stated by Learned Hand in *United States v. Carroll Towing Co.*, 159 F.2d 169, 173 (2d Cir. 1947).

businesses. All businesses should be encouraged to act responsibly and in this regard, Web site sponsors should be treated no differently from offline businesses. As previously noted, however, what is reasonable should depend upon the context, and a determination of reasonableness should factor in the ways that online businesses are different from offline businesses. Finally, a "reasonableness" standard best reflects social norms and accommodates technological evolution, making it especially attractive in the dynamic online context.

The proposals in this Article will not banish all online harassment, nor will they stop the most determined trolls; however, the proposals do force Web site sponsors to recognize there are measures they can take to curb abusive and damaging conduct on their Web sites. Cyberharassment is just too easy on the Internet. Perhaps most important, these proposals recognize and treat online harassment as the social problem that it is, rather than assuming all conduct and postings on the Internet are constitutionally protected "speech."

The underlying objective of these proposals is to more closely align the social norms that exist on the Internet with those in the physical world. While many free speech advocates decry any sort of regulation as "censorship," that term is wrongly applied where the content regulators are private entities. In fact, proactive steps on the part of Web sites may have the effect of forestalling government intervention efforts that could be more sweeping and invasive than actions taken by Web site sponsors, and certainly more restrictive than the foregoing proposals. For example, the federal grand jury indictment and conviction of Lori Drew in the high-profile MySpace cyberharassment case has generated much consternation among legal experts.[241] Because there was insufficient evidence to bring charges under state criminal statutes, federal prosecutors brought the indictment under the Computer Fraud and Abuse Act.[242] The indictment stated the Act was violated when Drew violated MySpace's terms of service.[243] Several legal scholars argued that the

---

[241] *See* David Ardia, *Lori Drew Indicted for Misuse of MySpace in Megan Meier Suicide Case*, http://www.citmedialaw.org/blog/2008/lori-drew-indicted-misuse-myspace-megan-meier-suicide-case (May 16, 2008); Duclos, *supra* note 159; Orin Kerr, *The MySpace Suicide Indictment—And Why It Should Be Dismissed*, http://volokh.com/posts/1210889188.shtml (May 15, 2008, 18:06 PDT); Daniel Solove, *Is The Computer Fraud and Abuse Act Unconstitutionally Vague?*, http://www.concurringopinions.com/archives/2008/05/is_the_computer.html (May 22, 2008, 14:29 PDT); Daniel J. Solove, *Megan Meier Case Update—Drew Indicted*, http://www.concurringopinions.com/archives/2008/05/megan_meier_cas.html (May 15, 2008, 17:46 PDT); Kim Zetter, *Experts Say MySpace Suicide Indictment Sets "Scary" Legal Precedent*, http://blog.wired.com/27bstroke6/2008/05/myspace-indictm.html (May 15, 2008, 17:39 PDT).

[242] Kim Zetter, *Judge Postpones Lori Drew Sentencing, Weighs Dismissal*, WIRED.COM, May 18, 2009, http://www.wired.com/threatlevel/2009/05/drew_sentenced (May 18, 2009). A federal judge later overturned the jury's guilty verdicts. Kim Zetter, *Judge Acquits Lori Drew in Cyberbullying Case, Overrules Jury*, WIRED.COM, July 2, 2009, *available at* http://www.wired.com/threatlevel/2009/07/drew_court/.

[243] *Id.*

prosecution set a dangerous precedent because few people read Web site terms of service. [244]

VI. CONSTITUTIONAL SCRUTINY OF PROPOSED ANTI-CYBERHARASSMENT POLICIES

The First Amendment is often used as a defense to online harassment claims.[245] Part VI addresses the First Amendment doctrine in the online context generally, and then specifically as it pertains to the "reasonable measures" proposed in Part IV.

A. The Awkwardness of Applying First Amendment Doctrine to Online Harassment

The First Amendment prohibits the government from impinging on the freedom of speech. The objective of this prohibition was to prevent censorship and to encourage a free marketplace of ideas, which in turn, leads to knowledge and truth.[246] Yet there are limitations on the free speech right. These limitations include defining what constitutes "expression." Obscenity, for example, is deemed to have no real expressive value and is not considered "speech" protected under the First Amendment.[247] Certain crimes and torts, such as verbal assault, defamation, and perjury, are directed purely at certain types of speech.[248]

Whether words in a given context are protected as "speech" under the First Amendment may be analyzed in terms of the public/private distinction. Although

---

[244] *See id.*; *cf.* Nick Akerman, *The Law Fits the Crime*, NAT'L L.J., May 26, 2008, at 1; Kim, *supra* note 162. In Korea, the suicide of a popular actress, reportedly distressed over Internet rumors, has prompted the governing party to promote a law to punish online insults that would be tougher than existing laws. *See* Choe Sang-hun, *Korean Star's Suicide Reignites Debate on Web Regulation*, N.Y. TIMES, Oct. 13, 2008, at B7.

[245] *See* N.Y. Times Co. v. Sullivan, 376 U.S. 254, 276–77 (1964) (holding that the First Amendment limits recovery for defamation).

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

[247] *See* Davenport v. Wash. Educ. Ass'n, 551 U.S. 177, 188–89 (2007) (noting that "speech that is obscene or defamatory can be constitutionally proscribed because the social interest in order and morality outweighs the negligible contribution of those categories of speech to the marketplace of ideas").

[248] *See* E. Walter Van Valkenburg, *The First Amendment in Cyberspace*, 75 OR. L. REV. 319, 319 (1996) ("[P]rotections afforded by the First Amendment . . . are far from absolute. Certain categories of communication are subject to extensive regulation and, in some cases, outright prohibition. Defamation, for example, can give rise to civil liability, as can communication that violates rights to privacy or publicity. Pornography and other forms of obscenity are, under well established law, outside the protections of the First Amendment.").

public speech is said to be accorded more protection than private speech,[249] harms that are framed as "public" harms are also weighted more heavily than those that are framed as "private" harms.[250] For example, where speech is labeled as obscene and not protected expression, the harm is to community norms. Defamation injures one's reputation,[251] which is the way others—the social community—think about the plaintiff, not the personal injury that it has caused the plaintiff.

In addition to criminal laws that limit speech, there are competing rights that limit free speech. Copyright, trade secret, and trademark law limit what one can say and/or how one can say it. With each of these, the right holder's interest is pecuniary and therefore "public" because it affects the marketplace, rather than "private," where the injury would be limited to the affected individual.

The Internet poses unique challenges and requires us to rethink the way we define rights and harms when it comes to speech.[252] Where speech is "obscene," courts have asked whether there was any expressive value and whether and to what extent community norms of decency were offended.[253] Yet how do we evaluate speech against community norms where both the community and the norms are uncertain?[254] What is the community for purposes of Internet speech?[255] If poster

---

[249] *See* Connick v. Myers, 461 U.S. 138, 146 (1983) ("When employee expression cannot be fairly considered as relating to any matter of political, social, or other concern to the community, government officials should enjoy wide latitude in managing their offices, without intrusive oversight by the judiciary in the name of the First Amendment.").

[250] Another way to consider the public/private distinction is as a power dynamic, given that those with a "public" interest have more socioeconomic power. For example, the movie industry is more powerful than an individual, and individuals belonging to minority groups have even less power. As Richard Delgado and Jean Stefancic have pointed out, "[p]owerful actors . . . have always been successful at coining free speech 'exceptions' to suit their interest." Richard Delgado & Jean Stefancic, *Ten Arguments Against Hate-Speech Regulation: How Valid?*, 23 N. KY. L. REV. 475, 484 (1996). For further discussion on this issue, see *Davenport*, 551 U.S. at 188–89 (noting "speech that is obscene or defamatory can be constitutionally proscribed because the social interest in order and morality outweighs the negligible contribution of those categories of speech to the marketplace of ideas").

[251] *See* State v. Carpenter, 171 P.3d 41, 51 (Alaska 2007) (explaining that a defamatory statement "'tends to harm the reputation of another so as to lower [her] in the estimation of the community or deter third persons from associating or dealing with [her]'") (quoting Briggs v. Newton, 984 P.2d 1113, 1120–21 (Alaska 1999)); Nguyen-Lam v. Cao, 171 Cal. App. 4th 858, 867 (Cal. Ct. App. 2009) (noting that "defamation constitutes an injury to reputation"); *see also* RESTATEMENT (SECOND) of TORTS § 559 (1977).

[252] *Cf.* Van Valkenburg, *supra* note 248, at 324 (observing that "existing First Amendment doctrine should translate relatively well to Cyberspace").

[253] *See Davenport*, 551 U.S. at 118 (citation omitted).

[254] *See* Branscomb, *supra* note 20, at 1652 (discussing the problem of deciding "which local community's standards should apply—that of the uploading provider, that of the downloading user, or the community standards maintained by and within the virtual community on the electronic network" in an online pornography case).

"X" describes sexual acts he would like to do to poster "Y," such communication may be considered obscene in certain communities but not in others. The unrestrained nature of online discourse may lower the bar of socially acceptable speech on a particular Web site, which then spills over to other Web sites. Often what is considered obscene in an offline context is considered the norm on a particular Web site or chat room.[256]

Significantly, the norms on the Internet are now being shaped, and the extent to which we permit certain types of behavior affects what those norms are.[257] Uncivil and even unlawful conduct is perceived as a right. For example, stolen digital images of a movie star were posted online.[258] The actor had taken his computer to be serviced, and the employees of the computer services firm had helped themselves to the contents of his digital photo album.[259] When the police conducted an investigation, many online comment posters decried a crackdown on the right to free speech.[260] But when did publication of stolen personal photographs constitute a free speech right?[261]

Many of the existing limitations on the right to speech do not apply in the context of the Internet. Courts have permitted reasonable time, place, and manner restrictions even with protected speech. The Internet blurs the public/private distinction and makes traditional time, place, and manner restrictions inapposite. For example, X, our hypothetical online harasser, is at home typing in the middle of the night, not on a street corner during the working day.

The purpose of time, place, and manner restrictions is to provide for public safety and to maintain order. Yet a secondary effect of the restrictions is to filter out those speakers who have only an impulsive or trivial interest in making a statement. In the offline world, there are physical barriers and pragmatic limitations to speech that are absent in the virtual world.[262] For example, a speaker

---

[255] *Cf.* John Fee, *Obscenity and the World Wide Web*, 2007 BYU L. REV. 1691, 1691 (arguing it is "constitutionally permissible to apply the traditional test for obscenity, the *Miller* standard, to the Internet, including its reference to 'contemporary community standards,' without any requirement for a more particular definition"). Fee argues against using a different standard for the Internet because doing so would "tip the scales" in obscenity cases toward defendants. *Id*. at 1692.

[256] But as Danielle Citron notes, "anonymous message-board postings are not immune from defamation liability simply because they are too outrageous to be believed." Citron, *supra* note 12, at 108.

[257] *See* Branscomb, *supra* note 20, at 1641.

[258] Keith Bradsher, *Internet Sex Video Case Stirs Free-Speech Issues in Hong Kong*, N.Y. TIMES, Feb. 13, 2008, at C3.

[259] *Id.*

[260] *Id.*

[261] This example is even more striking considering the actor was Chinese and the comment posters appeared to be from China, which does not have free speech rights as in the United States. *See id.*

[262] Harry Surden, *Structural Rights in Privacy*, 60 SMU L. REV. 1605, 1606 (2007) (noting that society relies upon latent structural constraints to inhibit unwanted conduct in a

may want to make a statement about the war in Iraq, but she may not feel strongly enough about making that statement to drive down to City Hall and join a demonstration on a rainy day. In addition, an individual who wishes to express an opinion in the physical world must find an outlet that finds that opinion newsworthy, or at least valuable to its readers. That opinion is thus subject to some sort of editorial screening, and the circulation of that publication often correlates with the selectivity of that screening process. Of course, an individual may also self-publish an opinion via leaflets or by shouting that opinion through a bullhorn. In those cases, the circulation of that opinion will be limited in both territory and duration. Leaflets are not preserved (if they are even read), and the existence of an opinion shared using a bullhorn does not survive its transmission. In addition, distribution of leaflets and the use of bullhorn announcements are subject to the time, place, and manner restrictions mentioned above.[263]

Some may argue that the very benefit of the Internet is its democratic accessibility.[264] While this may be so, it does not diminish the argument that Internet communication is not treated the same as communication in the physical world. The physical barriers and legal restrictions placed on speech in the physical world serve as a means by which to screen out impulsive speakers and false or misleading information; Internet postings are not subject to the same built-in delay or editorial process. Postings can be made in the heat of emotion, without deliberation or a second opinion, and without a cooling period. The susceptibility of Internet communications to impulsive behavior is made even more significant given that the age of users appears to correlate strongly with frequency and complexity of online activity.[265] Data collected from a survey conducted in August 2008 by the Internet and American Life Project of the Pew Research Center notes that 38 percent of people age 65 and older use the Internet compared with 91 percent of those ages 18 to 29, 86 percent of those ages 30 to 49, and 74 percent of

---

way that is functionally comparable to the law, and discussing how these latent structural constraints are vulnerable to dissipation due to emerging technologies).

[263] Lucero v. Trosch, 121 F.3d 591, 599 (11th Cir. 1997) (holding abortion protestors were properly prohibited from demonstrating, including using bullhorns, within 200 feet of the residences of abortion clinic staff).

[264] *See* SOLOVE, *supra* note 74, at 20, (arguing that "[b]logs are more egalitarian than the mainstream media" because "[y]ou don't need connections to editorial page editors to get heard. If you have something interesting to say, then you can say it"). Solove discusses the thrill of the blog:

> The blog I posted on was visited thousands of times a day. A lot of people were reading. What made this so exciting was that I'd never had any success getting an op-ed published. I had tried many a time, but the editors just wouldn't give me a plot of valuable space on their pages. Suddenly I no longer needed them.

Id. at 5.

[265] *See infra* notes 266–268 and accompanying text.

those ages 50 to 64.[266] Even within a narrow age range, such as college students, the younger students were found to be more likely to post their creations online.[267] Not surprisingly, some online posters may experience "poster's regret,"[268] a wasted emotion when the damage has already been done.

The proposals in Part IV contemplate how Internet communication differs from communication in the physical world.[269] The public/private distinction has affected free speech analysis in a way that is inapplicable to Internet speech. Much of free speech analysis considers the location of where speech occurs and whether the defendant has a "commercial" interest in the speech. Commercial is typically understood to mean that the defendant has a pecuniary stake in the action rooted in the speech defense, such as a copyright or a valuable trade secret. With respect to online harassment, the competing interests are between the speaker and the object of the speech, and to a lesser extent, the site visitor's "right to know."

Much of the harm caused by distribution might be avoided if we limited anonymity.[270] Anonymity has been tied to free speech, but limiting anonymity in the context of online harassment has positive "public" effects. Restricting anonymity increases reliability of information and encourages accountability, respects the public's interest in the source of the information, heightens the expressive value of the speech, and reinforces social/community norms.

The private harm created by online harassment also has harmful public effects. Cyberharassment affects the employability of victims of harassment, undermines community norms, and ignores the malleability of such norms, thus leading to the "lowest common denominator" effect (i.e., a speaker's conduct lowers the standard of civility on a Web site). It affects the way we interact with others, introducing a type of distrust and paranoia into personal relationships that may ultimately make such intimacy difficult, if not impossible. It also affects our expectations and our sense of what is normal and acceptable, creating incremental changes to our culture whether we acknowledge it or not. Because so many of the existing available tort remedies depend upon normative standards, such as

---

[266] Pew Internet & American Life Project, Demographics of Internet Users, http://www.pewinternet.org/Trend-Data/Whos-Online.aspx (2009).

[267] Eszter Hargittai & Gina Walejko, *The Participation Divide: Content Creation and Sharing in the Digital Age*, 11 INFO. COMM. AND SOC'Y. 239, 249–53 (2008).

[268] *See* Emily Gould, *Exposed—What I Gained—and Lost—By Writing About My Intimate Life Online*, N.Y. TIMES MAG., May 25, 2008, at 32 (discussing the emotional repercussions from blogging intimate details); Witt, *supra* note 36 (chronicling the aftermath of blogger Jessica Cutler's exposure by another, widely read blog). For a discussion of how social norms address individual problems of willpower and self-control, see Katherine J. Strandburg, *Privacy, Rationality, and Temptation: A Theory of Willpower Norms*, 57 RU. L. REV. 1235 *passim* (2005).

[269] S. Elizabeth Malloy, *Anonymous Blogging and Defamation: Balancing Interests of the Internet*, 84 WASH. U. L.R. 1187, 1192 (2006) (noting that the Internet is different from other mediums in its ease of access, permanence, and pervasiveness).

[270] For a more comprehensive discussion of the costs and benefits of anonymous speech, see Lidsky & Cotter, *supra* note 116, *passim*.

reasonableness, they may fail to protect the very values that those standards were intended to reflect. While some types of online harassment may now seem shocking or unexpected, repeated reports of such conduct may diminish that effect. For example, pictures of nude celebrities or celebrities having sex were shocking when they first appeared on the Internet; now, such images are commonplace and easy to find. A failure to explicitly address online harassment may dull our sensitivity to it. Resignation to cultural changes, however, should not be confused with acceptance or receptiveness. In the end, we must acknowledge that some types of communication or speech are just not expressive (or not expressive of anything that our society and judiciary have deemed worthy of protection).

The standard First Amendment response to "bad speech" has been "more speech."[271] This response makes certain assumptions about "bad speech" that are inaccurate or unproven. First, it assumes that "bad speech" is in fact constitutionally protected speech. It also assumes that "more speech" will be accorded the same platform as "bad speech," and that any response will be distributed widely enough to blunt any ill-effects from the "bad speech."[272] In fact,

---

[271] *See* Wolf, *supra* note 118 ("[T]the best antidote to hate speech, ADL maintains, is more speech."). Kurt Opsahl, a staff attorney at the Electronic Frontier Foundation, notes that for those who feel slandered, "[T]the cure to bad speech is more speech." Nakashima, *supra* note 2.

[272] Professor Andrew Chin makes the convincing argument that because of concerns about balkanization and concentration of power exaggerated by the use of external Web links, the Internet is "one of many fora where social structure constrains public discourse." Andrew Chin, *Making the World Wide Web Safe for Democracy: A Medium-Specific First Amendment Analysis*, 19 HASTINGS COMM. & ENT. L.J. 309, 313 (1997). Chin uses the following illustration:

> [S]uppose that there are two perspectives, A and B, with respect to a particular political issue. Perspective A is held by 40% of the public and Perspective B is held by 10%, with the remaining 50% undecided. Each perspective is represented by a number of sites on the Web, proportional to its level of support in the population. Suppose that proponents of B believe that their perspective will be persuasive to anyone who engages in a deliberative comparison between A and B. Web sites for B therefore include many links to Web sites for A. On the other hand, proponents of A may believe that the best way to protect their lead in the polls is to avoid any reference to B. Because there are many more A sites than B sites on the Web, publishers of A sites can be confident that their perspective will be seen by the undecided reader.
>
> As a result of these strategies, Web sites for A actually garner *more than* four times as many hits as Web sites for B among exploring readers. . . . This situation is analogous to the plight of marginalized groups in conventional public discourse: the minority group, in order to survive, must understand the dominant perspective sufficiently to deconstruct and criticize it, whereas the mainstream group may benefit unjustly from its ignorance of minority perspectives.

a site constructed by someone unfamiliar with how search engines retrieve results may get little or no attention at all.[273] College students have been found to be heavily influenced by the order in which Google search results were presented.[274] These students exhibited substantial trust in Google's ability to rank results by their relevance to the query even where the abstracts were less relevant to their query.[275] Thus, to effectively respond to bad speech, one must have the resources and know-how to effectively distribute that response as widely as the initial posting.

Finally, the "more speech" rejoinder fundamentally misunderstands the nature of "bad speech." Although speech that expresses unpopular or reprehensible views may indeed be addressed or diluted by "more speech," speech that threatens or personally attacks an individual is quite different. Responding to personal attacks by an anonymous poster through "more speech" adds fuel to the fire and may result in more vicious and repeated attacks. For example, when the parents of a boy with Keppen-Lubinsky syndrome (a rare congenital disorder), protested that images of their son were being distorted and circulated on the Internet, one Web site provided the following response:

> Instead of locking this grotesque sin against the natural order in a dark basement like they should have, his family maintains a website chock full of lulzy photographs of the abomination as if they were actually proud of pushing the bawling skinbag out of the mother's obviously cursed twat.
>
> His parents, however, were operating under the false assumption that the internets is a happy place where everyone's feelings are respected and validated. It comes as no surprise then that the proud parents were shocked, SHOCKED, when they discovered that photos of their son had exploded across the internet into a wide variety of lulzy photoshoops and macros.[276]

Id. at 315–16. *See also* Citron, *supra* note 12, at 67 (stating online, anonymous mobs target traditionally subordinated groups, such as women, people of color, religious minorities, gays, and lesbians).

[273] *See* Oren Bracha and Frank Pasquale, *Federal Search Commission? Access, Fairness, and Accountability in the Law of Search*, 93 CORNELL L. REV. 1149, 1151 (2008) (discussing "'search engines' power to manipulate their results, thereby affecting the ability of Internet communicators to reach potential audiences"); James Grimmelmann, *The Structure of Search Engine Law*, 93 IOWA L. REV. 1, 6–14 (2007) (discussing how modern search engines function); Tushnet, *supra* note 15, at 993 (noting that on the Web "there remain substantial concentrations of power over public discourse").

[274] *See* Bing Pan et al., *In Google We Trust: Users' Decisions on Rank, Position, and Relevance*, 12 J. COMPUTER-MEDIATED COMM. 801, 816 (2007).

[275] *Id.*

[276] Encyclopedia Dramatica, *supra* note 33. I include these statements to illustrate the aggression that a response to harassing posts might elicit. Although these statements might arguably constitute parody and/or protected expression, they might also constitute

The Web site continues its abuse by calling the boys' parents "un-intelligent un-washed Guidos (as if there are any other kind), [who] have difficulty grasping the basics of the English language."[277] The insults are accompanied with doctored photographs of the boy and hurtful captions mocking his condition.[278]

In addition to aggravating attacks, a requirement that the victim of an attack respond to the attack with "more speech" further degrades the victim by forcing him or her to engage the attacker. A response by the victim may also lend the initial attack more legitimacy and draw more unwanted attention to the post.

One could argue that recipients of online harassment should simply ignore the harassment and "grow a thicker skin."[279] The problem with this suggestion is not simply that it is unrealistic, but also that it encourages us as a society to cultivate insensitivity and apathy as a norm, and to shun mutual respect and civility as core values. Inaction to the problem of online harassment does not simply maintain the status quo. On the contrary, it protects and reinforces a standard of conduct that would be intolerable in the physical world. Even differentiating the "virtual world," or "cyberspace," from the "offline world," or the "physical world," is problematic because it assumes the existence of two different universes or realities. As this Article reflects, I am highly critical of this assumption. I nevertheless use the terms to distinguish Internet activity from non-Internet activity, a distinction that is important given the unique dimensions of harassment where the Internet is used as a medium of communication. In other words, although the Internet is not a different universe, communication distributed via the Internet has different effects from communication distributed through other mediums. This Article is concerned

---

intentional infliction of emotional distress, particularly when viewed in conjunction with the digitally altered images of the boy.

[277] *Id.*

[278] *Id.*

[279] For example, law professor and blogger Ann Althouse criticized the filing of the AutoAdmit lawsuit by stating: "So this is the 21st century? Where courts award punitive damages for offensive words and pictures? Isn't 'the scummiest kind of sexually offensive tripe' exactly what we always used to say people had to put up with in a free country? Man, that was so 20th century!" Ann Althouse, *Yale Law Students Sue Over the 'The Scummiest Kind of Sexually Offensive Tripe' at AutoAdmit*, http://althouse.blogspot.com/2007/06/yale-law-students-sue-over-scummiest.html (June 12, 2007, 15:52). In reference to commentary about Althouse's post, another law professor and blogger, Glenn Reynolds, added:

> Well, I'm pretty thick-skinned about Internet trash-talk—when I teach libel I give my students a few choice search terms and let them see what people have said about me. They're usually appalled, but I've never sued anyone, and the list of things about which I might actually sue is awfully short. Besides, once you get past the puppy-blending stuff, who's going to believe much of anything they read?

Glenn Reynolds, *Suing AutoAdmit*, http://www.pajamasmedia.com/instapundit-archive/archives2/006203.php (June 12, 2007, 19:26 PDT).

with the effects of Internet communication without meaning to suggest that those effects are confined to the Internet. The remainder of Part VI explains how and why the strategies proposed in Part IV, with a few modifications, survive constitutional scrutiny.

B. Contractual and Architectural Constraints are Content-Neutral

The contractual and architectural constraints proposed in Part IV are intended to curb impulsive and regrettable behavior by forcing the poster to think before pressing send. The effect may be to evaluate and filter speech, but it is the poster, and not a government actor, who is censoring communication. These contractual and architectural constraints serve some of the same functions as time, place, and manner restrictions and structural barriers. They provide an opportunity for contemplation without imposing a ban on speech, leaving the decision whether to post the communication in the hands of the poster. A state-mandated policy might arguably adopt even more onerous content-neutral restrictions without violating free speech principles.[280] I do not advocate broader restriction, but raise the possibility simply as a point of comparison—as an example of how far the government could go in the absence of self-imposed regulation on the part of both Web site sponsors and users.[281] My proposed contractual and architectural constraints, by contrast, merely encourage the exercise of best judgment and self-control.

C. Easy Unmasking Proposals Can Be Limited to Survive Constitutional Scrutiny

Although the Supreme Court has recognized that the First Amendment protects a general right to anonymity, it has done so in limited contexts and only after weighing governmental interests against individual interests.[282] The Supreme Court has never ruled on an absolute right to anonymity,[283] nor has it ruled on the

---

[280] *See* Perry Educ. Ass'n v. Perry Local Educators' Ass'n, 460 U.S. 37, 44–55 (1983).

[281] Content-neutral government regulations are subject to a less rigorous analysis than content-based regulations. *See* Turner Broad. Sys., Inc. v. F.C.C., 520 U.S. 180, 213–15 (1997).

[282] Talley v. California, 362 U.S. 60, 64–65 (1960) (striking down as unconstitutional a city ordinance prohibiting the distribution of handbills without identifying the sponsors); McIntyre v. Ohio Elections Comm'n, 514 U.S. 334, 357 (1995) (holding that Ohio statute banning distribution of anonymous political campaign literature was not justified by state interest in preventing fraud and libel and informing voters).

[283] In *Talley v. California*, the city ordinance prohibited all anonymous leafleting. 362 U.S. at 60. In *McIntyre v. Ohio Elections Commission*, the text of the state statute contained no language limiting its application to fraudulent, false, or libelous statements, and therefore the Court held it was overbroad. 514 U.S. at 357.

issue of anonymous speech regarding nonpublic matters.[284] In fact, language in the two Supreme Court cases recognizing a constitutionally protected right to anonymity suggest it would not extend to false or fraudulent speech.[285] Furthermore, although Internet anonymity has been recognized by lower courts,[286] the Supreme Court has never addressed the issue of whether anonymity on the Internet is constitutionally protected, much less decided upon the parameters of any such presumed right.

"Easy unmasking" policies do not mandate identification as a precondition to posting, nor do they prohibit anonymous speech. Furthermore, policies where unmasking is limited to cases of online threats, gossip, and confessionals typically would not involve protected speech.[287] Easy unmasking in these three situations is unlikely to affect protected speech because they involve threats or defamatory statements. Even if the gossip or confessionals involve events or facts that are true, they may be invasive of privacy because they publicly disseminate private information about private individuals. Finally, governmental regulations or court decisions may avoid First Amendment challenges by making easy unmasking policies voluntary, but also encouraging their adoption. For example, the adoption of an unmasking policy may be evidence of reasonable care, but a failure to adopt such a policy in and of itself would not constitute negligence.

D. Prohibition on Certain Digital Images is Narrowly Tailored to a Legitimate Government Interest

There are anticipated objections to the outright prohibition of digital images of non-public figure children and of nude individuals. The first objection is that they limit the expression of the poster. In the case of images of nude individuals, many of these images would not be considered fully protected speech because they would be obscene or pornographic and could be regulated under the government's police power.[288] The expressive nature is debatable as the poster is not the subject

---

[284] The decision in *Talley* addressed an economic boycott, 362 U.S. at 60, and the decision in *McIntyre* dealt with political speech, 514 U.S. at 334. *See also* Strickland, *supra* note 80, at 1558 (asserting that a "thorough examination of both *McIntyre*'s facts and the Court's analysis indicates that the assumption that the case extends to all anonymous Internet speech is conclusory and may be incorrect," and that "wholesale application of *McIntyre* in the context of a cybersmear claim is misapplied").

[285] *See McIntyre*, 514 U.S. at 1523 (noting that the right to anonymity may be abused when it shields fraudulent conduct and that the state may punish fraud directly); *Talley*, 362 U.S. at 538 (expressly noting that the Court was not deciding on ordinances limited to prevent fraud).

[286] *See* Doe v. 2TheMart.com Inc., 140 F. Supp. 2d 1088, 1097 (W.D. Wash. 2001).

[287] Of course, Web site sponsors could apply unmasking strategies to a wider range of conduct.

[288] *See* Heideman v. S. Salt Lake City, 348 F.3d 1182, 1195–96, 1183 (10th Cir. 2003) (holding ordinance banning nudity within sexually oriented business was not subject to strict scrutiny because prohibition was on a form of conduct and applied to all such

in the photograph; the act of expression then is the uploading of another's image.[289] Even where speech is affected, the government has a compelling state interest in protecting citizens' most basic privacy. There is indisputably a privacy interest at stake where unauthorized, widespread distribution of nude images is concerned, especially where the subject is not a public figure.

The government has a compelling state interest in protecting minors from abuse and exploitation. Some Missouri lawmakers are considering an outright ban on sex offenders' permission to take photographs of children primarily because of the ease with which such photographs can be shared with other sex offenders on social networking sites.[290] Georgia lawmakers have also considered a similar measure.[291] Yet recent studies indicate that online harassment of teens by their peers is a bigger threat than sexual predation online.[292] Cyberharassment by peers includes not just images taken without the consent of the subject, but images taken by the subject him or herself, which are then misused by the recipient.

According to a recent study, one in five teenagers and one in three young adults use cell phones and online technology to send or post nude or seminude images of themselves.[293] Seventy percent of those who admitted to sending sexual images of themselves sent them to a boyfriend or a girlfriend.[294] A teenager sending a sexy image to a significant other is not thinking the relationship might meet an unpleasant end. In the aftermath of a breakup, teenagers and young adults may not be thinking rationally. Raging hormones, a bruised ego, and a brain not yet fully formed in the crucial ability to empathize and control emotions make possession of an ex's naked digital image a powerful and dangerous weapon. With a few clicks of a mouse, a jilted and heartbroken teen can get the type of revenge that was unimaginable a few years ago. Although young love does not last forever, a digital image of one's naked teen self might, haunting someone like a digital

---

businesses, including those not engaged in expressive activity). In fact, section 230 expressly does not apply to statutes criminalizing obscenity and child pornography. *See* 47 U.S.C. § 230(e) (2006).

[289] Furthermore, nudity is not in and of itself expressive. *See* City of Erie v. Pap's A.M., 529 U.S. 277, 294 (2000).

[290] Keith Chrostowski, *Missouri Lawmakers Ponder a Ban on Sex Offenders Photographing Children*, PRIMEBUZZ, Feb. 12, 2008, http://primebuzz.kcstar.com/?q=node/10022.

[291] *Id.*

[292] *See* INTERNET SAFETY TECHNICAL TASK FORCE, ENHANCING CHILD SAFETY AND ONLINE TECHNOLOGIES, (2008), *available at* http://cyber.law.harvard.edu/sites/cyber.law.harvard.edu/files/ISTTF_Final_Report-Executive_Summary.pdf; *see also* Melissa Healy, *My Pal, My Bully; Kids' Online 'Friends' Can Be Far from Friendly*, L.A. TIMES, Jan. 26, 2009, at F1 (describing the finding of a Harvard University-led task force that children on social networking Web sites are relatively safe from adult predators but more likely to experience psychological trauma from online harassment by peers).

[293] Survey, National Campaign to Prevent Teen and Unwanted Pregnancy & Cosmogirl.com, Sex and Tech: Results from a Survey of Teens and Young Adults 1, http://www.thenationalcampaign.org/sextech/PDF/SexTech_Summary.pdf.

[294] *Id.* at 4.

scarlet letter and limiting one's future career choices and life opportunities. News stories and court cases indicate young men are more likely to exact this type of revenge upon their ex-girlfriends.[295] In addition, more than 80 percent of survey respondents said they thought the reason girls send sexy images is to get a guy's attention (compared with 60 percent who thought guys did so to get a girl's attention) and about 40 percent said they thought girls sent sexy images under pressure from a guy (compared with 18 percent who thought guys did so under pressure from a girl).[296]

The restriction on speech imposed by this Article's proposed ban on these two categories of digital images is narrowly tailored to the specific harms created by widespread and easy Internet distribution. It does not prohibit existing avenues for distribution, such as print publication. It is also limited to publicly accessible Web sites and would not preclude someone from posting photographs to an invitation-only, password-required, photo-sharing Web site. The restriction on speech—if these images would qualify as protected speech—applies only where the necessary consent is missing. As previously mentioned, the poster can always digitally alter or crop out an objecting subject's image in an otherwise permissible image, such as a group picture. Clear parameters could be established on response times or the number of requests required before determining that the Web site sponsor has acted unreasonably. Concerns that a Web site might be inundated with illegitimate takedown requests might be tempered if requestors were fined for failing to provide verification of their identities and standing to request the takedown. Finally, a court might conclude that reasonable conduct entails only taking down images of nude nonpublic figures, rather than any unauthorized nude image.[297]

---

[295] *See Laure Manaudou*, CHI. TRIB., Aug. 11, 2008, http://www.chicagotribune.com/sports/olympics/chi-laure-manaudou-080811-ht,0,6552632.story (describing how nude photos of Laure Manaudou, an Olympic swimmer from France, appeared on Web sites after a tempestuous break-up with her boyfriend). The photos appeared to have been taken by a lover in "an intimate moment," but her boyfriend disclaimed any responsibility. *Id.* Manaudou reported that, "[w]henever I typed Laure Manaudou on the Internet, it was horrible. I felt humiliated." *Id.*; *see also* Barnes v. Yahoo!, No. Civ. 05-926-AA, 2005 WL 3005602 (D. Or., Nov. 8, 2005), *rev'd*, No. 05-36189, 2009 WL 1232367 (9th Cir., May 7, 2009) (addressing plaintiff's complaint over ex-boyfriend posting nude pictures of plaintiff to Yahoo's online profiles).

[296] *Id.* at 2.

[297] Constitutional law scholar Erwin Chemerinsky has noted U.S. Supreme Court cases "try to strike a balance: They give more weight to speech that is relevant to the political process and of public interest; they give more weight to reputation when a person has not voluntarily entered the public domain and when the matter is not of public concern." CHEMERINSKY, *supra* note 150, at 1055. Another potential objection to a ban is that the image is the property of the individual who captured it, since that individual owns the copyright. This argument should also be dismissed because copyright ownership should not be allowed to trump the privacy and security interests at stake in these two limited circumstances. Copyright is granted to encourage creators to create for the benefit of society; yet it is not socially beneficial to have unauthorized pictures of minors or unauthorized pictures of naked children or adults circulating on the Internet. It is unlikely

VII. CONCLUSION

Although there are difficulties in monitoring content, Web sites should not then have no obligation to deter or minimize online harassment on their Web sites. Whether one concludes that Web sites are sui generis or "just like property" is beside the point. Web site sponsors have a proprietary interest in their sites and should have some accountability for what happens as a result of the forum they provide (even if not the same liability that mainstream media publishers have). This Article proposes several simple measures Web sites can take to deter online harassment without having to pre-screen or make subjective decisions about user-supplied content. By suggesting actions that Web site sponsors can readily adopt, this Article aims to shift the normative expectations of Web site sponsor behavior and to reframe the problem of online harassment as one of a failure of business norms rather than of free speech gone wild.

---

that prohibiting the dissemination of these two categories of images without consent would deter creators from pursuing photography or videography of other types of images or of those images in other contexts. In fact, some copyright holders may actually support such a measure as it might limit unauthorized Internet distribution of their copyrighted works. For a discussion of copyright and pornography, see Ann Bartow, *Pornography, Coercion, and Copyright Law 2.0*, 10 VAND. J. ENT. & TECH. L. 799, 837 (2008) (proposing "a copyright law framework that conditioned enforceability upon performer consent," which would enable performers to "leverage copyright protections to curtail commercial distribution of works they appeared in as a consequence of coercion").