Website Proprietorship and Cyber Harassment

Nancy Kim, California Western School of Law
While 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 aggravate the nature of harassment on the Internet. Furthermore, Section 230 of the Communications Decency Act provides website sponsors with immunity for content posted by others and no incentive to remove offending content.

Given the unique nature of cyber harassment, ex post punitive measures are inadequate to redress grievances. In this Article, I propose the imposition of proprietorship liability upon website sponsors who fail to adopt “reasonable measures” to prevent foreseeable harm, such as cyber harassment. I also introduce several proposals to deter cyber 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

Introduction
I. What Is Cyber Harassment?
   A. Verbal Cyber Harassment
      1. Cyber Threats
      2. Cyber Insults
      3. Cyber Gossip
      4. Cyber Confessions
      5. Cyber Deception.
      6. Cyber Terrorism
   B. The Use of Images in Cyber Harassment
   C. An Overview of Existing Remedies
      1. Tort Actions Deriving From the Right To Privacy
      2. Other Torts
      3. Crimes
II. The Need for Alternative Approaches to Cyber Harassment
   A. The Inadequacy of Existing Remedies.
   B. The Awkwardness of Applying First Amendment Doctrine to Cyber Harassment.
III. Increasing Website Accountability
   A. Encouraging Self-Regulation
   B. Imposing Proprietorship Liability Upon Website Sponsors
   C. Imposing Proprietorship Liability Conforms To Objectives of Tort Law
IV. Proposals to Address the Problem of Cyber Harassment
   A. Contractual and Architectural Constraints
      1. Manifesting Assent to Website Policies.
      2. Indemnification for User Misconduct.
      3. Community Controls.
      4. Default To Identified Postings.
      5. “Cooling Period.”
   B. Ameliorating Anonymity’s Negative Effects
      1. Easy Unmasking Of Anonymity
      2. Stigmatizing Anonymity
   C. Prohibition of Certain Digital Images
V. Constitutional Scrutiny of Proposed Anti-Cyber Harassment Policies
   A. Contractual and Architectural Constraints Are Content Neutral
   C. Prohibition on Certain Digital Images Is Narrowly Tailored To a Legitimate Government Interest
Conclusion
WEBSITE PROPRIETORSHIP AND CYBER HARASSMENT

INTRODUCTION

Several female law students were the subject of malicious and pornographic comments on AutoAdmit, a website catering to law school students.\(^1\) The cruel nature of the posts, the hostile, unrepentant mob mentality of the anonymous posters and the adamant refusal of the website operators to remove the offensive posts shocked the legal community and attracted media attention.\(^2\) After repeated unsuccessful requests to the website operator to remove the posts, two of the women sued, claiming that the posts caused them emotional distress and harmed their professional opportunities.\(^3\) As part of the litigation, the identities of several of the posters were revealed.\(^4\) One of the named defendants was later dropped from the case and then sued the plaintiffs, alleging emotional distress and damage to his professional reputation.\(^5\)

The AutoAdmit case illustrates the damage that cyber harassment wreaks upon the subjects of the harassment as well as the harassers. While the harm to targets of online smear campaigns is obvious what is less discussed is that the harassers also risk damage to their reputations.\(^6\) While online communication is often phrased as expressive speech, the nature of online discourse is often shaped by the website itself. For example, the founder of AutoAdmit marketed the website as an alternative to other message boards

---


\(^2\) Id.

\(^3\) Id.

\(^4\) Id.

\(^5\) Id.

\(^6\) One of the defendants in the AutoAdmit case claimed that the lawsuit has ruined his life. Another one claims that he has been unable to find a job as a result of the negative publicity surrounding the website and the litigation. Margolick, *supra* note 1.
that filtered out inflammatory posts.\(^7\) This Article adopts a new approach to the problem of cyber harassment by treating it primarily as a failure of business norms rather than as a matter of unfettered speech.

The term “cyber harassment” 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).\(^8\) Other words capture unsavory Internet conduct. “Cyber stalking,” for example, is the term most frequently used to describe the threatening and often anonymous stalking of an individual through chat rooms, email and instant communication.\(^9\) Some forms of cyber harassment are not persistent or threatening as much as annoying or humiliating. Some commentators distinguish “cyber harassment” from”cyber bullying” by defining cyber harassment as directed at adults and cyber bullying as directed at students or children.\(^10\) But the range of conduct and/or communication makes the use of one term inadequate. The absence of precise terminology makes discussion of the problem of cyber harassment difficult. Consequently, proposals aimed at one type of conduct may be inappropriate (either under- or over-inclusive) for other types of conduct.

In this paper, I use the term “cyber harassment” as a general term to characterize the use of the Internet as a medium for disseminating harmful material about another individual. The definition is deliberately loose in order to accommodate different types of

\(^7\) Margolick, *supra* note 1.
\(^8\) While harassment of a social or political group or organization, such as racial or religious minorities, constitute cyber harassment, this Article focuses specifically on harassment targeted at individuals.
conduct. In this paper, I argue that the social problem of cyber harassment is one that
should be addressed by website sponsors. By “website sponsor,” I refer to the companies
and individuals which own the URL and that conduct business or other activity on the
website; I am not referring to Internet service providers or other web hosting companies
(ISP’s) such as GTE that technically enable those businesses, unless those companies
also sponsor the site or own the domain name (such as AOL, which provides Internet
access but also sponsors its own message board). ISPs are usually not in a position to
control website content. Furthermore, the volume of traffic that a single ISP transports is
typically many times greater than that hosted by any single website sponsor.
Accordingly, different standards should apply to ISPs and website sponsors and I confine
my discussion in this Article to website sponsors.

Framing cyber harassment as a private sector problem resolves or reduces many
of the free speech concerns raised by First Amendment advocates.\footnote{This is not to suggest that government regulation is not an appropriate way to address the problem of cyber harassment, 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. Private law remedies should be viewed in conjunction with—not as exclusive of—public law approaches. For a discussion of a cyber civil rights strategy, see Danielle Keats Citron, \textit{Cyber Civil Rights}, 89 B.U. L. Rev. (forthcoming 2009) (arguing that cyber harassment harms ought to be understood and addressed as civil rights violations).} It empowers and
encourages website sponsors to shape developing norms as part of good business
practices. Setting expectations for user conduct empowers website sponsors to better
control their website 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 among users regarding expectations of conduct on a
particular website.
In addition, courts should impose tort liability upon website sponsors for creating unreasonable business models. To hold website sponsors accountable for creating socially irresponsible websites applies the same standards to Internet proprietors as currently applies to offline proprietors, albeit with allowances for the differences between Internet and offline proprietorships (such as dramatically higher volume online). Currently, website sponsors exercise power over their websites 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 importantly, despite their ability to control site content, website sponsors are immune from liability as publishers under Section 230 of the Communications Decency Act of 1996 (“CDA”). Courts have generally interpreted this provision to grant broad immunity to website sponsors. Section 230 thus places responsibility for content directly – and exclusively -- upon those who create it and absolutely relieves from liability the websites which profit (or hope to profit) from it. Yet, the immunity granted to them under Section 230 as publishers should not mean that website sponsors should be free from all liability for harm arising from their businesses. Courts should treat website sponsors like other proprietors and hold them accountable for irresponsible and harmful business practices.

Cyber harassment is often viewed through the prism of free speech. Any attempt to curb the substance of what is being said online, is automatically elevated to a

---

12 The Ninth Circuit expressed its concern with applying different rules for offline and online businesses when it stated that “we must be careful not to exceed the scope of the immunity provided by Congress and thus give online businesses an unfair advantage over their real world counterparts, which must comply with laws of general applicability.” Fair Housing Council of San Fernando Valley v. Roomates.com, LLC, 521 F.3d 1157, 1162 n.9 (9th Cir. 2008).
14 Rebecca Tushnet notes that the CDA uncouples ISP “property” ownership from responsibility. Tushnet, supra note 61, at 1016. Tushnet proposes that Internet intermediaries’ immunity should be tied to limits on their ability to control speech. Id. at 1015.
discussion of constitutional rights. Furthermore, online “speech” is analyzed in the same way as offline “speech.” Yet, online communication is not the same as offline communication. While harassment and bullying have always existed, when such behavior is conducted online, the consequences have different dimensions. The anonymity of harassers, the ease of widespread digital dissemination, and the inability to contain and/or eliminate online information change the nature of harassment when it is conducted on the Internet. Much of the discussion of online harassment assumes that such “speech” is just like offline speech, and thus subject to the same First Amendment protections. By focusing on the action as “speech,” assumptions are made about what speech is that bias the analysis. In other words, using the rhetoric of free speech uncritically assumes that all Internet communication is protected expression.

Although this paper proposes several strategies that website sponsors can implement to reduce the incidence of cyber harassment, it does so with the awareness that any solution must be flexible enough to accommodate technological evolution. The primary objective of this paper is not to provide all-encompassing, immutable solutions to cyber harassment; rather, it is to propose a new way of looking at what is, in fact, a new and evolving problem. Cyber harassment is not “just like” harassment offline. To apply existing free speech doctrine without recognizing those differences ignores the normative-shaping impact of Internet communication at this stage of technology adaptation and accommodation.\(^{15}\) While my proposals do not eliminate all forms of

\(^{15}\) This is not to say that there are not legitimate free speech concerns that are implicated by 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 (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 (2006) (advocating the formation of state-sponsored websites that would constitute public forums for free speech).
cyber harassment on all websites, they do encourage moving away from the impulsive, “anything goes” culture which prevails on some websites 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-slopist First Amendment absolutism. Thus one objective of this Article, is to reconcile the culture of the Internet with offline social norms of behavior.

In order to avoid solutions that are overbroad, the problems they are intended to address must be specifically delineated. In Part I, I identify and describe the various types of conduct which fall under the umbrella definition of “cyber harassment.” In this Part, I also provide a brief overview of legal doctrines which are currently used to address the problem of cyber harassment.

In Part II, I explain why the existing remedies are inadequate to resolve the problem of cyber harassment. In Part III, I summarize and further develop an argument that I first proposed elsewhere, that tort law and, in particular, a liability analogous to premises or business owner liability, may effectively be used to impose standards of conduct upon website sponsors. I propose that the adoption of the anti-cyber harassment proposals set forth in Part IV (or similar proposals), should constitute the “reasonable measures” that website sponsors should take to protect their users from cyber harassment.

In Part IV, I propose some “reasonable measures” that website sponsors should take to reduce the incidence of cyber harassment on their sites. The proposals offered in

---


17 A premises-liability argument has been rejected by courts. I discuss the leading case rejecting premises liability and why the court’s grounds for rejecting the theory was wrong in Part III.
this section focus on deterring cyber harassment rather than penalizing such conduct. The proposals also take into consideration the ways in which web-based businesses are different from bricks-and-mortar businesses. In particular, given the high volume of traffic handled by web proprietors, they do not impose pre-screening obligations or require the proprietor to make subjective decisions regarding whether to remove user supplied content.

I conclude that the problem of cyber harassment necessitates a change in the way we currently view the role of website sponsors. Website sponsors are proprietors of businesses, not state-sponsored public forums. Some website sponsors have accepted the responsibilities that come with proprietorship by creating safeguards and designing websites that discourage unlawful activity. Other website sponsors, however, have intentionally adopted business models and designed their websites in a way that encourages cyber harassment. While they may be immune from liability as publishers for harmful content on their websites, they should be held liable as proprietors for the creation of businesses that were likely to cause harm to third parties.

I. What Is Cyber Harassment?

The very usefulness of the phrase cyber harassment as a broad, catch-all term makes it necessary to categorize the various types of conduct that fall under it. For example, cyber harassment covers both repeated and unwanted email 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 and the intended and likely effect upon the victim of the harassment vary. Accordingly, the solutions to prevent, deter or punish such actions should also vary. A failure to delineate and categorize different types of conduct risks policy proposals and solutions that are overbroad or otherwise ill-suited for some problems, although appropriate for others.

A useful characterization of forms of cyber harassment must recognize that words and images may be employed in a variety of ways and to different effects. While cyber harassment can occur in closed arenas, such as through email or closed group invitations, I limit my discussion in this Article to cyber harassment that is conducted on publicly accessible websites, including those sites that are open to members only, if membership is non-selective and available to anyone who applies. Certain online communication (e.g. emails and list serve communications and invitation-only websites 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 further in Section II, publicly viewable and searchable information has the potential to cause greater harm than restricted websites.

18 For the sake of brevity, I will refer to those websites, such as social networking sites, that require membership as “publicly accessible” where the contents of those sites are available to all members and membership is non-selective. In other words, if the contents are available only to invited viewers, then that site, or portion of that site, is not publicly accessible. If the content are accessible if one registers with the site, but registration is automatically granted, then that site is publicly accessible for the purposes of this Article.

19 Cyber harassment on closed websites also causes harm to its victims; however, to avoid being overbroad, this Article focuses on problems that are particular to publicly accessible websites. For example, “invitees” to password protected sites are not members of the general public and my analysis and
In this section, I provide a description of the various forms of cyber harassment which divides the harassing conduct into two general categories, verbal and visual/auditory. This will then be the terminology that I use to discuss proposed solutions.

A. Verbal Cyber Harassment

Words convey meaning in cyberspace but not necessarily in the same way as in the physical world. Words may be used to communicate intent to harm another, or they may be used simply as a way to express oneself, in a way that incidentally harms another.

1. Cyber Threats

The expression of intent to inflict harm constitutes a “cyber threat” where such expression is communicated through the medium of the Internet. Cyber stalking is a pattern of repeated cyber threats.

2. Cyber Insults

Cyber insults are words that are used to offend, deride or embarrass another. Cyber insults differ from cyber threats because the object or subject of the attack 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. A Cyber insult would include opinions about an individual or an occurrence involving that individual.

3. Cyber Gossip
-Women are encouraged to anonymously post information on a public website about their exes, including that they are promiscuous, have sexually transmitted diseases, and have illegitimate children.\textsuperscript{20}

-An anonymous user posts on a popular social networking site that another family in the neighborhood has a son (identified by name) who “has been to jail” and dates “underaged girls.”\textsuperscript{21}

Cyber gossip is the spreading of rumors or personal information about others. Cyber gossip is distinguishable from cyber insults because it is presented as “factual”. Cyber gossip includes both rumors that are later substantiated as accurate as well as falsehoods.

4. \textit{Cyber Confessions}

-A blogger revealed explicit sexual information about her identifiable partners, including that one enjoyed being spanked, another was married and that a third paid her for sex.\textsuperscript{22}

- The wife of a Broadway mogul revealed 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.\textsuperscript{23}

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

5. \textit{Cyber Deception}.

\textsuperscript{20}See Don’tDateHimGirl.com; see also http://www.nytimes.com/2006/02/16/fashion/thursdaystyles/16WEB.html?scp=3&sq=Don%27t%20date%20him%20girl%20website&st=cse
A thirteen year old girl committed suicide after communicating with a woman, who was posing as a teenaged boy through a fake MySpace account.\(^{24}\)

A man posing as a woman posted an ad on a popular message board seeking a “brutal dom muscular male.” He then listed the names, pictures, email addresses and phone numbers of the men who responded to his blog.\(^{25}\)

On the Internet, as the oft-quoted New Yorker cartoon states, nobody knows that you’re a dog.\(^{26}\) In some cases, the ability to disguise oneself and masquerade as someone else has led to tragic consequences.\(^{27}\) The ease of hiding one’s true identity and the use of communication tools to forge relationships make cyber deception especially devious, especially given that sometimes there is no crime for the resulting emotional wrongs.\(^{28}\)

6. **Cyber Terrorism**

In some cases, harassers take action that goes beyond communicative activity. Cyber terrorism is the use of intimidation in a systematic way to achieve a particular objective, other than pure communication. Cyber terrorists may hack into a victim’s email 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 website or blog.\(^{29}\)

---

27 See Jennifer Steinhauer, *Verdict in MySpace Suicide Case*, N.Y. TIMES, Nov. 26, 2008 (forty-one-year-old woman disguised as teenaged boy resulted in suicide of teenaged girl).
28 Id. (noting that there was no existing crime under Missouri law for cyber deception).
29 For example, Kathy Serra, a blogger and software developer, was attacked on her own blog and on other websites. Posters revealed her home address and Social Security number. See Jessica Valenti, *How the Web Became a Sexists’ Paradise*, THE GUARDIAN, Apr. 6, 2007; Citron, *supra* note 10, at 3-4.
B. The Use of Images in Cyber Harassment

-A pedophile frequented parks and playgrounds, took pictures of young children, and posted them to his website, accompanied by sexually suggestive comments.

-School children surreptitiously snap pictures of their classmates undressing during gym class and post the photographs to a public website.\(^{30}\)

-A group of children force a classmate to engage in humiliating acts while videotaping him. The video is then posted to a public website for other classmates to view.\(^{31}\)

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

-A jilted boyfriend vengefully posted nude pictures of his ex-girlfriend online.\(^{32}\)

Cyber harassment may involve the use of images, such as photographs or videos. While the method by which such images are captured may vary, for purposes of my analysis, all images – whether captured as a photograph, video or document – are classified simply as images. Images may accompany a cyber confession. For example, an individual may post a video of herself talking about an impending divorce.\(^{33}\) In such cases, the words spoken by the individual should be viewed as a cyber confession and the video image (of the individual or others) should be analyzed as distinct from her cyber confession. An image often reveals more information, and 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)

\(^{30}\) See INTERNATIONAL ONLINE CONFERENCE REPORT, NEW FORMS OF SCHOOL BULLYING AND VIOLENCE 9 (Apr. 24-May 19, 2006) (on file with author).

\(^{31}\) Id.

\(^{32}\) Richard Morgan, Revenge Porn, DETAILS magazine, November 2008, p. 96.

\(^{33}\) 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 Jan. 4, 2009).
than posting his picture. Furthermore, as discussed in Section V, the posting of certain images should not be equated with speech protected by the First Amendment.

C. An Overview of Existing Remedies

Laws currently address some (but not all) of the crimes that now fall under the umbrella definition of cyber harassment. This Part C 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 background to frame the proposals offered in Section IV. Generally, the remedies currently available to victims of (some) types of cyber harassment can be grouped in three broad categories: tort actions deriving from privacy; non-privacy tort claims such as defamation and intentional infliction of emotional distress, and criminal or anti-stalking statutes.

1. Tort Actions Deriving from the Right to Privacy

The primary remedies for victims of cyber harassment derive from the right to privacy. In their groundbreaking article, Samuel Warren and Louis Brandeis first recognized privacy as a legal right. 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

---


35 Samuel Warren & Louis Brandeis, The Right to Privacy, 4 HARV. L. REV. 193 (1890). While the concept of privacy existed prior to publication of Warren and Brandeis’ article, the article is widely acknowledged as being the first to establish the legal foundation for such a right. See Solove, A Taxonomy of Privacy, supra note 26; Katherine Strandberg, Privacy, Rationality, and Temptation: A Theory of Willpower Norms, 57 RUTGERS L. REV. 1235, 1267-68 (2005)
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.\footnote[36]{Warren & Brandeis, \textit{supra} note 27, at 193.}

As many scholars have noted, however, while courts have recognized the existence of a “right to privacy,” the parameters of such a right are vaguely defined.\footnote[37]{Daniel J. Solove, \textit{Conceptualizing Privacy}, 90 \textit{Cal. L. Rev.} 1087 (2002) (discussing the problems with conceptualizing privacy and suggesting a new pragmatic approach that focuses on privacy problems) [hereinafter Solove, \textit{Conceptualizing Privacy}].

The recognition of a right to privacy\footnote[38]{\textit{Restatement (Second) of Torts}, § 652A (“One who invades the right of privacy of another is subject to liability for the resulting harm to the interests of the other.”).} gave rise to several common law actions in tort, namely appropriation,\footnote[39]{\textit{Restatement (Second) of Torts} § 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.”); Castro v. \textit{NYT Television}, 851 A.2d 88 (N.J. Super. Ct. 2004).} false light,\footnote[40]{\textit{Restatement (Second) of Torts} § 652E (“One who gives publicity to a matter concerning the private life of another that places the other before the public in a false light is subject to liability to the other for invasion of his 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.”).} disclosure or wrongful publication of private facts,\footnote[41]{\textit{Restatement (Second) of Torts} § 652D (“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.”).} and intrusion.\footnote[42]{\textit{Restatement (Second) of Torts} § 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.”).} Causes of actions based upon privacy torts would be most appropriate where the plaintiff was the subject of cyber confessions, cyber gossip and cyber insults.

2. \textit{Other Torts}

Defamation law protects the interests of a person in his or her reputation.\footnote[43]{See \textit{Hearst Corp. v. Hughes}, 466 A.2d 486 (Md. Ct. App. 1983).} In order to establish liability for defamation, the plaintiff must show that the defendant made a false and defamatory statement that harmed the plaintiff’s reputation.\footnote[44]{\textit{Restatement (Second) of Torts} §§ 558-59.} There are
two types of defamation torts, libel and slander. Libel is the publication of defamatory statements by printed or written words.\textsuperscript{45} Slander is the publication of defamatory matter by spoken words or by any form of communication other than those covered by libel.\textsuperscript{46} Defamation based causes of action would be appropriate where the plaintiff is the subject of cyber gossip, cyber insults, and cyber confessionals provided that the statements made were untrue. Ironically, the wild, juvenile nature of much online discourse itself may save it as the context may indicate that it should not be taken seriously (although it may nevertheless tarnish the reputation of the subject of the cyber harassment).

In addition, the object of the cyber 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.\textsuperscript{47} While the intentional infliction of emotional distress may provide a basis for all kinds of cyber harassment, it is particularly useful with cyber deception which occurs more frequently and in situations that are unique to the Internet compared to offline cases of false identity.

3. \textit{Crimes}

In addition to torts, cyber threats and/or cyber stalking may also be a crime.\textsuperscript{48} Typically, the defendant must have engaged in a behavior or a pattern of conduct, the

\textsuperscript{45} \textsc{Restatement (Second) of Torts} § 568.
\textsuperscript{46} \textit{Id}.
\textsuperscript{47} \textsc{Restatement (Second) of Torts} § 46 (“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.”).
\textsuperscript{48} \textit{See, e.g., Cal. Civ. Code} § 1708.7 (describing the tort of stalking, including cyber stalking, 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”); \textsc{Cal. Penal Code} § 422 (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
intent of which was to alarm, abuse or frighten the victim.\textsuperscript{49} Acts of cyber terrorism may be criminalized under anti-hacking statutes.\textsuperscript{50}

\section*{II. The Need for Alternative Approaches to Cyber Harassment}

This Part II explains why the existing remedies are inadequate to address the problem of cyber harassment. I then propose reframing the problem of cyber harassment as a failure of business norms rather than as a constitutional right to expression. I suggest that cyber harassment can be combated by changing expectations of the role that website sponsors play and by imposing tort liability on those who fail to meet those expectations. Website sponsors maintain a proprietary interest in their websites and we should expect them to conform to the standard of conduct expected of other proprietors.\textsuperscript{51}

A. The Inadequacy of Existing Remedies.

Cyber harassment is different in both the process by which it occurs, and the harms that it creates. While the existing remedies discussed in Part I.C. may adequately address offline harassment, for several reasons they are inadequate to deal with cyber harassment.

First, posting is cheap and easy. This aspect of web postings has two effects when it comes to cyber 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 even to those without substantial financial

\textsuperscript{49} See CAL. CIV. CODE \textsection 1708.7; CAL. PENAL CODE \textsection 422. See also ALA. CODE \textsection 13A-11-8; Harassment by Electronic Communication, H.R. 12, 23d Leg. (Alaska 2003); MASS. GEN. LAWS ch. 265, \textsection 43; Texas SB 1139, OHIO REV. CODE \textsection 2917.21(B).

\textsuperscript{50} See, e.g., 18 U.S.C. \textsection 1030.

\textsuperscript{51} Black’s Law Dictionary defines proprietor as “(a)n owner, esp. one who runs a business.” BLACK’S LAW DICTIONARY (8\textsuperscript{th} ed. 2004).
resources. Consequently, even where a plaintiff prevails in a civil action against a cyber harasser, the odds are high that the plaintiff will not be able to recover significant damages.

Furthermore, cyber harassment affects private individuals in a very public manner in a way that was previously infeasible. Because posting is cheap and easy, many forms of cyber harassment are more likely to involve a non-public figure than offline forms of the same conduct. For example, cyber insults and cyber gossip about non-public figures is much more common than publication of insults and gossip about non-public figures in traditional media. Unfortunately, because litigation is costly, many private individuals who are the target of cyber harassment don’t have the financial resources to pursue legal remedies. For example, the female law student plaintiffs in the AutoAdmit case mentioned at the beginning of this Article can afford to bring a lawsuit against their aggressors because they are being represented for free by one of the country’s leading litigation firms and one of the country’s leading intellectual property lawyers.\(^\text{52}\) It is unlikely that they would have done so otherwise for while the plaintiffs are seeking monetary damages, they will probably not receive much considering the defendants are likely students and/or recent graduates.\(^\text{53}\)

Second, many harassing posts are anonymous. Anonymity removes many of the social controls which may have deterred offenders in the pre-Internet era.\(^\text{54}\) Anonymity

\(^{52}\) Margolick, \textit{supra} note 1. \\
\(^{53}\) \textit{Id.} \\
\(^{54}\) \textit{See} \textbf{Daniel J. Solove, The Future of Reputation: Gossip, Rumor and Privacy on the Internet} 140 (2007) [hereinafter \textit{Solove, The Future of Reputation}] (noting that “[w]hen anonymous, people are often much nastier and more uncivil in their speech. 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
also reduces accountability and accuracy. Anonymous information is just 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 cyber gossip or cyber 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. 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.

Anonymity also reduces the likelihood of non-legal measures or conciliatory efforts. 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 non-legal manner. The victim of cyber harassment must initiate legal proceedings in order to unmask the identity of the poster as there is no other way to negotiate or respond to the posting, other than by responding via a post. In fact, anonymity removes any opportunity to redress grievances in a non-public manner. The untrustworthy and malicious. They might no longer share secrets with the person. They might stop believing what the person says.”

55 Justice Scalia made this argument in his dissent in *McIntyre v. Ohio Elections Commission*, 514 U.S. 334 (1995) (noting that “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.”). *SOLove, The Future Of Reputation*, supra note 46, at 462-64.


57 *Id.*
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. Even if the subject of the post prevails in a lawsuit, posts may remain online during the drawn out litigation, causing more emotional harm.

Third, near instantaneous widespread dissemination and the impossibility of recapturing distributed postings put cyber 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. Cyber insults, for example, are likely not libelous yet because of their widespread distribution and permanence, they are harmful in a way that offline insults are not.

The issue of whether the Internet is different from the offline world and necessitates different rules has been a recurring topic for discussion among academics and commentators. Perhaps the more relevant issue, at least regarding the problem of cyber harassment, is not whether the Internet is or is not 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 that they would not do in the offline world, something that psychologists refer to as the online “disinhibition effect”. Website sponsors routinely accept anonymous postings whereas

---

58 See John Suler, The Online Disinhibition Effect, THE PSYCHOLOGY OF CYBERSPACE, http://www-usr.rider.edu/~suler/psycyber/disinhibit.html; see also John M. Grohol, Teens, Sex and Technology,
none of the major newspapers accept anonymous op ed contributions or letters to the editor. Anonymous phone calls are not as credible as anonymous printed information. 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 which makes traditional responses to harassment inadequate. Website sponsors often disclaim all responsibility for harassing conduct that occurs on their website and many make no attempt to monitor or control uploaded content. If such conduct were to occur on physical property, for example, in a store, 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, the website is immune from liability under Section 230 of the CDA.59

The remedies currently available require a victim of cyber harassment to file costly, time-consuming and often fruitless lawsuits. While this may be a problem in the physical world, it is a greater problem in the virtual one because of the unique aspects – ease of publication, anonymity, widespread distribution and lack of control -- of Internet publication.

59 See Goddard v. Google, Inc., 2008 WL 5245490 (N.D. Cal. Dec. 17, 2008)(noting that courts “consistently have held that section 230 provides a “robust” immunity”); Carafano v. Metrosplash.com, Inc., 339 F.3rd 1119, 1123 (9th Cir. 2003)(doubts should be “resolved in favor of immunity”); Doe v. MySpace, Inc. 528 F.3d 413 (5th Cir. 2008); Barrett v. Rosenthal, 146 P.3d 510, 529 (2006)(noting that section 230 “does not permit” Internet service providers or users to be sued as “distributors.”)
B. The Awkwardness of Applying First Amendment Doctrine to Cyber Harassment

The First Amendment is often used as a defense to the existing causes of action which poses a significant complication to cyber harassment claims. The First Amendment prohibits the government from impinging upon 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. Yet, there are limitations on the free speech right. These limitations include defining what constitutes “expression.” Obscenity and pornography, for example, are deemed to have no real expressive value and are not considered “speech” protected under the First Amendment. Certain crimes and torts, such as verbal assault, defamation, and perjury, are directed purely at certain types of speech.

Whether words in a given context are protected as “speech” under the First Amendment may be analyzed in terms of the public/private distinction. While public speech is said to be accorded more protection than private speech, harms that are framed as “public” harms are also weighted more heavily than those that are framed as “private” harms. For example, where speech is labeled as obscene and not protected expression, the harm is to community norms. Defamation is defined as injury to one’s reputation, which is the way that others – the social community – think about the plaintiff, not the personal injury that it has caused the plaintiff.

---

60 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 that “[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 (1996).
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 re-think the way we define rights and harms when it comes to speech. Where speech is “obscene”, the courts have asked whether there was any expressive value and whether and to what extent community norms of decency were offended. Yet, how do we evaluate speech against community norms where both the community and the norms are uncertain? What is the community for purposes of Internet speech? If a poster [X] describes certain sexual acts that he would like to do to another poster [Y], such communication may be considered obscene in certain communities, but not in others. The unrestrained nature of online discourse further lowers the bar of social acceptability on a particular website which then spills over to other websites. Often what is considered obscene in an offline context is considered the norm on a particular website or chatroom.

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. Uncivil and even unlawful conduct is perceived as a right. For example, stolen digital images of a movie star were posted online. The actor had taken his computer to be serviced and the

---

61 Cf. John Fee, Obscenity and the World Wide Web, 2008 BYU L. REV. 1691 (2008) (arguing that 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.

employees of the computer services firm had helped themselves to the contents of his
digital photo album. 63 When the police conducted an investigation, many in cyberspace
decried a crackdown on the right to free speech. 64 But when did publication of stolen
personal photographs constitute a free speech right? 65

Many of the existing limitations on the right to speech don’t apply in cyberspace.
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 cyber harasser, is at
home typing in the middle of the night, not on a street corner during the working day.

The purpose of these time, place and manner restrictions is to provide for public
safety and to maintain order. Yet, a secondary effect of these restrictions was to filter out
those speakers who had only an impulsive or trivial interest in making a statement. In the
physical world, there are physical barriers and pragmatic limitations to speech that are
absent in the virtual world. 66 For example, a speaker 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 fill out a permit to speak at a designated time. 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
depends upon the selectivity of that screening process. Of course, an individual may also

63 Id.
64 Id.
65 This example is even more striking considering the actor was Chinese and the commenters appeared to
be from China which does not have free speech rights as in the United States.
66 Harry Surden, Structural Rights in Privacy, 60 SMU L. REV. 101 (2007) (noting that society relies upon
latent structural constraints to inhibit unwanted conduct in a way that is functionally comparable to the law,
and discussing how these latent structural constraints are vulnerable to dissipation due to emerging
technologies).
self-publish an opinion via leaflets or by shouting that opinion through a bull horn. 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 bull horn does not survive its transmission. In addition, distribution of leaflets and the use of bull horn announcements are subject to the time, place and manner restrictions mentioned above.

Some may argue that the very benefit of the Internet is its democratic accessibility. While this may be so, that doesn’t diminish the argument that Internet communication is not treated the same as communication in the physical world. The physical barriers and legal restrictions placed upon 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-off” 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. Data collected from a survey conducted in August 2008 by the Internet and American Life Project of the Pew Research Center notes that 38% of people aged 65 and older use the Internet compared to 91% of

---

67 Solove, for example, notes that blogs are “more egalitarian” than mainstream media: “You don’t need connections to editorial page editors to get heard. If you have something interesting to say, then you can say it.” Solove, The Future of Reputation, supra note 46, at 20. 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.
those aged 18-29, 86% of those aged 30-49 and 74% of those aged 50-64. Even within a narrow age range, such as college students, younger students were found to be more likely to post their creations online. As a recent study indicates, the teenage brain is still developing. The frontal cortex or the “thinking” part of the brain is growing and synaptically pruning itself. The prefrontal cortex, too, is undergoing 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. Not surprisingly, some online posters may experience “poster’s regret,” a wasted emotion when the damage has already been done.

In Section IV, I offer proposals to deter cyber harassment that take into consideration how Internet communication differs from communication in the physical world. 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

69 Eszter Hargittai & Gina Walejko, The Participation Divide: Content Creation and Sharing in the Digital Age, INFO., COMM. AND SOC’Y (forthcoming ) (manuscript at 13, on file with author).
70 Steve Connor, The teenage brain: A scientific analysis, THE INDEPENDENT, November 5, 2006 (discussing study by Dr. Sarah-Jayne Blakesmore of brain development of children using magnetic resonance imaging that indicates that areas of brain associated with higher level thinking and empathy are underused by teenagers).
71 Id.
72 Id.
74 S. Elizabeth Malloy, Anonymous Bloggers and Defamation: Balancing Interests on the Internet, 84 WASH. U. L.R. 1187, 1192 (noting that the Internet is different from other mediums in its ease of access, permanence, and pervasiveness).
secret. With respect to cyber 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.\textsuperscript{75} Anonymity has been tied to free speech but limiting anonymity in the
context of cyber 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 cyber harassment also has harmful public effects.

Cyber harassment 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
website). It affects the way that 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 much of the existing available tort remedies depend upon normative
standards, such as reasonableness, they may fail to protect the very values that those
standards were intended to reflect. While some types of cyber 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

\textsuperscript{75} For a more 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
(2007).
failure to explicitly address cyber 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, has deemed worthy of protection).

The standard First Amendment absolutist response to “bad speech” has been “more speech.” 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.” In fact, an unpopular site or one constructed by someone


77 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 Web 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 engaged 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 perspective. Id. 315-16. See also Citron, supra note 10 (stating online anonymous mobs target traditionally subordinated groups, such as women, people of color, religious minorities, gays and lesbians).
unfamiliar with how search engines retrieve results may get little or no attention at all.\footnote{See Rebecca Tushnet, \textit{Power Without Responsibility: Intermediaries and the First Amendment}, 76 GEO. WASH. L. REV. 986 (2008)(noting that on the Web “there remain substantial concentration of power over public discourse.”) \textit{Id.} at 993.} College students, for example, have been found to be heavily influenced by the order in which Google search results were presented.\footnote{Bing Pan, Helene Hembrooke, Thorsten Joachims, Lori Lorigo, Geri Gay & Laura Granka, \textit{In Google We Trust: Users' Decisions on Rank, Position and Relevance}, 12 J. COMPUTER MEDIATED COMM. 801 (2003) \textit{Id.} at 16.} 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.\footnote{\textit{Id.} at 16.} Thus, in order to effectively respond to bad speech, one must have the resources to effectively distribute that response as widely as the initial posting.

Finally, the “more speech” rejoinder fundamentally misunderstands the nature of “bad speech.” While 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 often results in harsher, more vicious and repeated attacks. In addition, a requirement that the victim of an attack respond to the attack with “more speech” further degrades the victim by forcing the victim to wallow at the attacker’s level. A response by the victim may also lend the initial attack more legitimacy and draw more unwanted attention to the post.

Some may argue that objects of cyber harassment should simply ignore the harassment and “grow a thicker skin.” The problem with this suggestion is not simply that it is unrealistic; it also 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 cyber 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 in that 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 in order 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, while the Internet is not a different universe, communication that is distributed via the Internet has different effects from communication distributed through other mediums. This Article is concerned with the effects of Internet communication without meaning to suggest that those effects are confined to the Internet.

III. INCREASING WEBSITE ACCOUNTABILITY

Many types of cyber harassment might be curtailed or prevented if we altered our expectations of website sponsors. While debate continues to rage regarding whether websites should be treated as tangible (real or personal) property, most websites disclaim responsibility for the conduct of their users on their website. Legal duties and social norms and values govern the sense of responsibility that most business owners feel over the conduct of their patrons on their physical property. Yet, the legal duties and social norms governing the responsibility of website sponsors over the conduct of their users is still evolving despite rhetoric purporting to establish clear parameters.
Arguments disclaiming website sponsor responsibility reflect a one-sided and rather socially irresponsible notion of the privileges of website sponsors. Significantly, this view is at odds with physical world expectations of business owners. In this section, I make two different arguments for why website sponsors should adopt the proposals set forth in the preceding section. Both of these arguments appeal to website sponsor self-interest. The first argument, which is more carrot than stick, is that greater website accountability enhances website sponsor ability to control its business and image. The second argument, which is more stick than carrot, is that website sponsors may already have liability under tort law to address cyber harassment on their websites. I address each of these arguments in turn below.

A. Encouraging Self-Regulation

Website sponsors often express reluctance to regulate communication among users for various reasons, including because it undermines the nature of their website. Many websites already have policies in place which mirror some or most of the proposals set forth in Part IV. The primary problem has been in the reluctance of some website

---

81 See website policies of craigslist, available at http://www.craigslist.org/about/terms.of.use (“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.”). See website policies of YouTube, available at http://www.youtube.com/t/terms (“YouTube reserves the right to decide whether Content or a User Submission is appropriate and complies with these Terms of Service for violations other than copyright infringement, such as, but not limited to, pornography, obscene or defamatory material, or excessive length. YouTube may remove such User Submissions and/or terminate a User's access for uploading such material in violation of these Terms of Service at any time, without prior notice and at its sole discretion.”). See website policies of MySpace, available at http://www.myspace.com/, (“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
sponsors to enforce their own policies. Even websites whose very business models seem to encourage harassing behavior have policies that prohibit cyber harassment. Website 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 website; yet admitted that his failure to do so meant that he “lost his website” to “parasites” and responsibility for the conduct of the User submitting any such Content.

See website policies of eBay, available at http://m.ebay.com/Pages/UserAgreement/US.aspx (“Without limiting other remedies, we 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.”). One popular law professor blogger, Brian Leiter, 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.


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 agree not to post content that is “unlawful, threatening, abusive, tortious, defamatory, obscene, libelous, or invasive of another’s privacy.” 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 them 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.

“freaks”. The prevailing ethos of the Web is a libertarian one. Any attempt to restrict speech or activity tends to be greeted with cries of free speech or censorship – even though the entity seeking to regulate the conduct or the speech is a private actor. For example, a recent video of Alaska governor and Vice Presidential candidate Sarah Palin’s former church, the Wasila Assembly of God, was removed from YouTube for “inappropriate content.” Internet users condemned YouTube’s actions as “censorship,” comparing the site with government censorship in China and advocating retaliatory measures against YouTube. Speech regulation by private entities, however, is not an infringement of free speech. The First Amendment prohibits the government, not private actors, from restricting speech. Yet, many website users have grown accustomed to thinking of the whole of the Internet as a public forum, rather than as privatized websites, and view attempts to restrict activity as censorship.

Website sponsors are in the best position to regulate communication on their websites given concerns about governmental restrictions of speech. 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

83 Margolick, supra note 1 (noting that even his “timid, belated attempts to weed out the worst abuses...prompted an open rebellion.”).
84 See SLOVE, THE FUTURE OF REPUTATION, supra note 46, 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.”).
86 This may be due, in large part, to the absence of public forum for communication. See Nunziato, supra note 13.
87 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.”).
speech has been firmly established in the physical world, there has been a shift in the attitude toward Internet communication, with many arguing that restrictions on posting on non-governmental websites amounts to suppression of free speech by the website sponsors. For example, AutoAdmit defended its controversial message board by saying that 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 thought they have.”

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 that equates speech regulation on non-governmental websites as censorship.

As private actors, website sponsors have greater freedom to shape the nature of 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, to the standards of conduct set by the trolls of cyberspace.

This misperception regarding the private nature of websites may be partly responsible for the “anything goes” culture that prevails on some websites on the part of some users. Because some users regard their ability to post and participate on a website

---

88 Nakashima, supra note 1.
89 This is not to suggest that government censorship of the Internet is not a concern, only that it is not a concern when the website sponsors themselves regulate the content, and not the government. 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, Court Blocks Access to YouTube in Turkey, INT’L HERALD TRIB., Mar. 7, 2007 (reporting that a court in Turkey ordered blockage of all access to YouTube after a video appeared on the videosharing website 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, N.Y. TIMES, Mar. 21, 2008, at B1 (discussing China and Turkey’s ban on the YouTube website). China banned access to YouTube after video clips were shown on the website which showed Tibetan monks being dragged through the streets by Chinese soldiers. Spencer & Delaney, supra.
90 A cyberspace “troll” is one who intentionally disrupts online communities. See Schwartz, supra note 21.
as their right, rather than a privilege that can be taken away, they may engage in conduct that ultimately damages the reputation and image of the website. MySpace, for example, received much negative public attention from the cyber deception incident which resulted in the suicide of a teenaged girl. YouTube, eBay and craigslist regularly fend off infringement claims because of illicit content uploaded by users. Facebook struggles with trolls who misuse information posted on member pages.

To elevate our expectations of website sponsor accountability adjusts user expectations of who controls website activity and content – and enhances the website sponsor’s ability to control its own image and brand. The guidelines and standards established by websites in their user agreement and policy might then be taken more seriously by users as the contractual requirements that they are. For example, Lori Drew knew that posing as a sixteen-year-old boy in order to deceive and manipulate another MySpace users was against the company’s policies, yet she did so anyway.\textsuperscript{91} eBay has an extensive user policy which prohibits selling items that violate third party rights.\textsuperscript{92} While eBay may have instituted this policy in order 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”.\textsuperscript{93} This policy helps set user expectations of what is permissible on the site, and also of when YouTube will remove site content. By explaining its policies and managing expectations upfront, YouTube is better able to protect its image and its brand.

\textsuperscript{91} See Nancy S. Kim, \textit{Playing by the Rules of the Cyber Playground}, \textsc{The Providence J}., July 4, 2008.
Website image and branding, in turn, often directly correlates to mainstream acceptability and corporate sponsorship. For example, rather than being known as a site for porn video clips, YouTube is now known for quirky and humorous clips on a wide range of topics, making it a better site for more advertisers. JuicyCampus went out of business in February 2009 due to a lack of advertising revenue. Whether the lack of advertising revenue was due to the negative publicity surrounding the website and the New Jersey investigation or simply the result of the economic downturn was the subject of much speculation.  

Marketed in the right way, some anti-cyber harassment measures may be viewed as features or website advantages. While some users may resist any imposition of restraints, others may appreciate their potential for deterring impulsive behavior that they may later regret. For example, Google recently introduced an optional Gmail feature called “Mail Goggles”, which incorporates contractual restraints to prevent embarrassing user behavior. The feature prompts a user with a popup window that asks, “Are you sure you want to send this?” when the user tries to send email during certain times (i.e. late night to early morning hours), where a user is more likely to be inebriated. Users are then required to solve several math problems before Google will permit the message to be sent.

---

96 Id.
97 Id.
Website sponsors should voluntarily adopt cyber harassment policies before Congress mandates them. In the aftermath of the MySpace case, legislators have proposed laws that would criminalize similar conduct, although some fear that the proposed laws are overbroad. Some commentators have suggested that section 230 of the CDA should be amended so that website sponsors receive a type of limited immunity based upon lack of actual notice, rather than absolute immunity. Others, however, have noted that a notice and take-down scheme may put website sponsors in the awkward position of having to make legal determinations of what constitutes defamatory or otherwise tortious material. While the focus of this Article is on private law approaches to cyber harassment, it is worth noting that the success of any such approaches may have the effect of curbing government regulation.

My suggested anti-cyber harassment proposals are intended to deter impulsive and regrettable behavior by forcing the poster to think before pressing send. While the effect may be to evaluate and filter speech, it is the poster, and not a government actor, who is censoring communication. They provide an opportunity for contemplation.

98 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 website sponsors. 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.”
100 Mark “Rizzn” Hopkins, Should There be a Law Against Asshats like Me?, MASHABLE, http://mashable.com/2008/06/09/asshats/ (fearing that pending legislation will have the effect of criminalizing posts criticizing celebrities and mainstream media).
101 See SOLOVE, THE FUTURE OF REPUTATION, supra note 46, at 149-60 (arguing that once a website is notified about a cyber harassment problem, it should respond to the problem or be liable); Bradley A. Areheart, Regulating Cyberbullies Through Notice-Based Liability, 117 YALE L.J. POCKET PART 41 (2007), http://thepocketpart.org/2007/09/08/areheart.html (arguing for ISP liability based upon a notice and take-down scheme based on actual notice).
102 See Citron, supra note 10.
without imposing a ban on speech, leaving the decision whether to post the communication in the hands of the poster. The government could arguably adopt even more onerous content neutral restriction without violating free speech principles. 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. 

While many websites work to minimize cyber harassment, other websites actively encourage such behavior. Rather than seeking a more commercially acceptable image, these websites craft an alternative niche for themselves as a place where users can malign other individuals. While carrot-like incentives may work for those websites striving for mass market acceptance and commercial appeal, some websites may need a more stick-like measure.

B. Imposing Proprietorship Liability Upon Website Sponsors

One such stick-like measure may be the imposition of tort liability upon website sponsors. Elsewhere, I have argued that proprietorship liability should be imposed upon website sponsors. I summarize, clarify and further develop that argument in this section. In a previous essay, I analogized the duty of website sponsors to bricks-and-mortar businesses and advocated the imposition of liability similar to the “premises”

---

103 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, *Zoning the Internet: A New Approach to Protecting Children Online*, 2007 BRIGHAM YOUNG U. L. REV. 1417; Cheryl B. Preston, *Making Family-friendly Internet a Reality: The Internet Community Ports Act*, 2007 BRIGHAM YOUNG U. L. REV. 1471

104 See also Rebecca Tushnet, *Power Without Responsibility: Intermediaries and the First Amendment*, 76 GEO. WASH. L. REV. 986 (2008)(arguing that “Congress is free, within rather broad limits, to determine an appropriate intermediary liability regime.”) Id. at 988

liability imposed on offline businesses. The analogy to premises liability is not a perfect one given the differences between cyberspace and the physical world, including the inability to draw secure boundaries and screen for potential harm. Yet, website sponsors are proprietors and exercise their control over their businesses in many ways. Website sponsors enforce their proprietorship over their websites by establishing terms of use in clickwrap or browsewrap agreements. Websites may capitalize on their proprietorship by selling user information to advertisers. They may also sell advertising space or products, such as tee-shirts, directly on their websites. They may receive a percentage of revenues that their users receive from the sale of products on their websites. They may also profit indirectly by using their websites as marketing platforms to reach a broad audience. They may then sell ancillary products or services, such as books or consulting services, to this audience.

Website sponsors should bear some responsibility for their actions. While some argue that websites are property and should be treated as such, others disagree. Even those who disagree that websites are “just like” property must recognize the fact that website sponsors maintain control over the content of the site (whether or not they choose to exercise that control), are in the best position to prevent harm to other users on the site.

and may profit from activity on the site (whether or not they choose to sell products on their site). Many of the concerns that critics of the website-as-property view raise pertain to the difficulties of delineating boundaries of intangible works. These concerns are inapposite where the activity at issue is limited to what happens on the website.

Sponsors of publicly accessible websites are the owners or “proprietors” of their website, whether that website is a blog, a gossip site, or a retail site. Along with ownership comes responsibility. Because their sites are publicly accessible (and again, this Article is limited to content only on publicly accessible websites), they are more akin to businesses than to private residences. While some sites sell product and are clearly “for profit,” other sites are less clearly commercial. Yet, even those sites that are not obviously retail-oriented may monetize their content in some way, either by selling ancillary products like tee-shirts, by selling advertising, or by using the site as a marketing vehicle to sell products, such as a novel, or services, such as consulting. In some cases, a website may intend to generate a large readership in the hopes of eventually selling out to a larger commercial entity. In this Article, I use the term proprietorship or proprietary interest to refer to the website sponsor’s business interest in the activity on the website, and to avoid the larger question of whether websites are the “property” of the website sponsor. Of course, any discussion of website sponsor liability must recognize the difficulties inherent in distinguishing cyberspace activities from those

---


41
taking place in a physical space, and the importance of tailoring remedies to respond to those difficulties.

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.109 This duty is not to insure 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.110 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 reasonable care where there was a failure to provide security personnel or adequate lighting in a parking lot.111 A California court held that the owners of a restaurant could be found negligent for failing to protect its customers where the layout of the restaurant required customers to stand in front of parking spaces with low barriers.112

The critical factor in determining whether there was a duty of care (a prerequisite to a finding of negligence) is foreseeability -- i.e. whether the business owner knew that

109 See Restatement (Second) of Torts § 344.


111 Murphy, 418 A.2d at 432. See also Restatement (Second) Torts § 344.

an assault was occurring or was about to occur on the premises.\textsuperscript{113} For example, in one case, a customer verbally threatened the plaintiff and was escorted out of the tavern.\textsuperscript{114} The tavern employees then allowed the abusive customer to reenter the tavern where the customer attacked the plaintiff.\textsuperscript{115} 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 café.”\textsuperscript{116}

Two different tests determine foreseeability.\textsuperscript{117} The first is the “prior similar incidents” test, where a duty arises where incidents similar to the harm at issue should have put the business owner on notice.\textsuperscript{118} The second test is the “totality of the circumstances” whereby the court examines not just whether there were prior similar incidents, but other factors, such as whether the business was located in a high crime area.\textsuperscript{119} The Restatement 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 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...

\textsuperscript{113} \textit{But see} Michael J. Yelnosky, \textit{Business Inviters’ Duty to Protect Invitees From Criminal Acts}, 134 U. Pa. L. Rev. 883 (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).


\textsuperscript{115} \textit{Id.}

\textsuperscript{116} \textit{Id.} at 364; \textit{see also} Bartosh v. Banning, 251 Cal. App. 2d 378 (1967).


\textsuperscript{118} \textit{Id.} at 548-49.

\textsuperscript{119} \textit{Id.}
to take precautions against it, and to provide a reasonably sufficient number of servants to afford a reasonable protection.  

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

In Doe v. MySpace, the court expressly declined to apply premises based liability to the internet context. In that case, the minor plaintiff sued the online social networking site, MySpace, after she was sexually assaulted. One of the plaintiff’s claims was that MySpace failed to implement basic safety measures to prevent sexual predators from communicating with minors on MySpace. The court rejected the argument, stating that plaintiff cited no precedent for treating a website as “virtual premises.” Yet the court opinion reveals that it was primarily concerned that what the plaintiff was seeking would impose an undue burden upon MySpace’s business:

“Plaintiff’s alleged 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

---

120 RESTATEMENT (SECOND) OF TORTS § 344, cmt. f (1965); Barker v. Wah Low, 19 Cal.App.3d 710, 714 (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 (Tex. 1998).

121 Id.

its tracks and close this avenue of communication, which Congress in its wisdom has decided to protect.”

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 website, and the minor’s knowing violation of those procedures, instead of explaining why premises based liability is wholly inapplicable on the internet. But consider this -- if MySpace had no safeguards and fifty-percent of teens using MySpace had been assaulted by sexual predators (even though they accurately stated their age during registration), would the court have reach 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. Yet, such a conclusion would be untenable.

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

---

123 *Id.* at 851.
124 The district court merely states that it “declines 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 extent to a website as a ‘virtual premises.’” *Id.*
125 MySpace currently sets the default for users aged 14 and 15 at “private” rather than “public,” so that their profiles are not searchable or viewable by anyone other than their named friends.
126 *Id.* at 850 (“It is quite obvious the underlying basis of Plaintiff’s claims is that, through posting on MySpace, Pete Solis and Julie Doe met and exchange 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 Plaintiff’s claims as directed toward MySpace in its publishing, editorial, and/or screening capabilities.”)
Internet based businesses may have millions of site visitors compared to bricks and mortar businesses which have a couple dozen; accordingly, the ability to successfully police virtual premises may be more elusive. A determination of what constitutes reasonable proprietership conduct should take into account the vast amount of traffic that passes through a website. While one attack in an underground parking lot may suffice to put a bricks 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 cyber harassment would not be enough to establish foreseeability on a website where there are thousands of daily postings.

While the cases addressing business owner liability concerned physical harm to invitees, there is nothing in the underlying rationale of these cases that would preclude non-physical 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 non-physical 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. But this remedy is

127 See Hellar v. Bianco, 111 Cal. App. 2d 424 (1952) (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., 148 Mass. 513 (1889) (defendant railroad held liable for posting in office libelous newspaper extract about plaintiff railroad broker for forty days). See also § RESTATEMENT (SECOND) OF TORTS § 577 (1977).

What Constitutes Publication

(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.

Id. But cf. Scott v. Hull, 259 N.E. 2d 160 (Ct. App. Ohio 1970) (finding failure of building owner or agent to remove defamatory graffiti on the outside of building is not grounds for defamation suit because building owner and agent did not engage in “positive acts,” such as inviting public into premises).
unavailable to plaintiffs alleging cyber harassment because of the immunity granted to website 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 a ping-pong ball drop from a passing airplane as part of a promotion.\(^{128}\) Each ball contained a certificate entitling the holder to a prize from the defendant store.\(^{129}\) The plaintiff went to the site of the promotion and was injured by the crowd that rushed to retrieve the fallen balls.\(^{130}\) 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.”\(^{131}\)

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 by a radio station listener who was participating in a promotional activity.\(^{132}\) The radio station conducted a contest which rewarded the first contestant to locate a traveling disc jockey.\(^{133}\) Two minors, in pursuit of the disc jockey, negligently forced the decedent’s car off the highway\(^{134}\). 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

\(^{128}\) F.W. Woolworth v. Kirby, 302 So. 2d 67 (Ala. 1974).
\(^{129}\) Id. at 68.
\(^{130}\) Id.
\(^{131}\) Id. at 71.
\(^{132}\) Weirum v. RKO General, 539 P.2d 36 (Cal. 1975).
\(^{133}\) Id. at 38.
\(^{134}\) Id.
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.”

As previously mentioned, website sponsors under the CDA are immune from liability for content posted by users on their websites. Congress, in passing this legislation, intended to encourage the development of the Internet and to protect “good Samaritan” ISPs from liability for blocking or screening obscene material. Court decisions, however, have applied the immunity provision too broadly. As a

135 Id. at 39.
136 See Communications Decency Act, 47 U.S.C. § 230(b) (“It is the policy of the United States to…promote the continued development of the Internet and other interactive computer services and other interactive media….”).
137 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 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).
138 See, e.g., Zeran v. America Online, Inc., 129 F.3d 327 (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 Lyrisa Barnett Lidsky, Silencing John Doe: Defamation and Discourse in Cyberspace, 49 DUKE L.J. 855 (2000)
consequence, the very section intended to protect websites to screen and remove offensive content is now being used as a shield by websites to actively encourage the posting of such content. For example, the founder of Juicy Campus, a now-defunct website that encouraged its college student users to post gossip, stated on the site blog, “Juicy Campus is the provider of an interactive computer service.” He cited section 230 to support his claims that, “Juicy Campus is immune from liability from content posted by users.” Another website encourages users to anonymously post gossip about others, and even suggests that they create false profiles. The purpose of one website is specifically to provide a forum where women can post negative information about the men they have dated. Other websites permit users to post sexually graphic videos and photographs of their cheating ex-lovers.

The imposition of proprietorship liability on website sponsors furthers the legislative intent of the CDA. The intent underlying CDA immunity, at least as interpreted by courts, is to both permit website sponsors to monitor content and relieve them of the burden of doing so. This intent is understandable given that, at least on some websites, the amount of content would make screening and filtering an onerous

---

139 Jeffrey Young, New Jersey Investigates Juicy Campus Gossip Site for Possible Consumer Fraud Violation, CHRON. HIGHER EDUC., Mar. 19, 2008.
140 The homepage of that website states the following, “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!” http://www.gossipreport.com/ It also encourages the posting of photos and videos to “really tell a story!” Id.
141 DontDateHimGirl.com
142 This type of online posting has its own name, “revenge porn.” See Richard Morgan, Revenge Porn, DETAILS, V. 27., No. 2, p. 96 (Nov. 2008)(noting that “an entire website…is dedicated to the genre; another one…has material…of a woman doing a striptease with the caption “She loved getting naked for her bf before cheating on him so he decided to send this to us to post!” Id.
responsibility. The imposition of proprietorship-based tort liability would not mean an obligation to screen or filter content as the website sponsor would not be liable for information posted by third parties. Nor would it require website sponsors to determine whether a particular post is defamatory or otherwise criminal or tortious. It is not the failure to remove the post in a takedown request that determines whether the website sponsor is negligent; rather, negligence is determined by whether the website sponsor took reasonable steps to prevent or deter foreseeable cyber harassment. While it may not be reasonable to expect a website sponsor to filter numerous messages prior to posting, it is reasonable to expect them to set up their websites and to establish and enforce policies to discourage cyber harassment. The standard for liability would be negligence based upon the nature of the business (including volume of traffic), not strict liability.

The determination of reasonableness and foreseeability must take into account the legislative intent behind section 230 and consider the nature of the website, including the number of daily visitors and the size of the business. A leanly staffed business such as craigslist, for example, which receives millions of daily visitors, should not be expected to make content-based decisions regarding user postings. Given Congress’ objectives in implementing section 230 and the vast amount of traffic on many websites, website sponsors generally should not be required to implement procedures to prescreen or make subjective determinations of the lawfulness of user-supplied content; they can, nevertheless, implement other reasonable procedures, such as those proposed in Section IV, that do not require prescreening or subjective decisions. For example, a website that has a cyber harassment policy which incorporated architectural constraints would not be

---

143 The popular online classified advertising website, craigslist, reportedly received more than ten million new notices in a typical month in 2006. See Brief of Defendant-Appellee craigslist, Inc. at 4, Chicago Lawyers’ Committee for Civil Rights Under Law, Inc. v. craigslist, Inc., No. 07-1101 (7th Cir. 2008).
liable in the event that a third party posted defamatory content about a user, nor would it
be liable for refusing to remove the content. A website sponsor, however, should be
liable for the harm that results from its negligence in setting up its website and for its
business model which fails to incorporate reasonable steps or safeguards to prevent or
minimize foreseeable cyber harassment. A determination of reasonableness should take
into account the resource limitations of the particular business and the amount of traffic
that passes through the website.

In order to establish that it has acted reasonably, website sponsors should adopt
policies and procedures, such as those set forth in Section IV to prevent or reduce the
likelihood of cyber 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-cyber harassment policies might indicate negligence.

Finally, a website should be liable for its conduct in responding to cyber
harassment complaints. For example, one of the female law students in the AutoAdmit
case emailed one of the website’s founders and requested that he take down certain
offensive posts about her. He responded in an AutoAdmit post and warned that if he kept
receiving similar requests, he would post them on the message board.144 While not liable
for the content of the posts by its users, 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). The plaintiff would have to establish harm before it
could charge that the website sponsor’s negligence was responsible for the harm;
however, it would be the website’s own actions for which it is liable. The possibility of
being subject to tort liability may prod website sponsors who are otherwise unwilling to

144 Margolick, supra note 1.
self-regulate into adopting policies and procedures to reduce or minimize cyber harassment.

C. Imposing Proprietorship Liability Conforms to Objectives of Tort Law

The call for greater website sponsor accountability is a call for a normative shift in the way we view cyber harassment. Requiring a certain level of accountability on the part of website sponsors is not particularly shocking. In fact, the call for website sponsor liability in this Article is less onerous than the standards imposed upon websites for posted copyrighted material.  

Website sponsors adopt a hypocritical position by claiming their websites are public forums and that they are constrained by free speech concerns from taking any action to prevent cyber harassment while at the same time aggressively treating their websites as “private property” for commercial gain. Of course website sponsors are at liberty to cater to their users’ preferences and desires, but in doing so, they should be held liable for their users’ abuses. The business models of certain websites are specifically intended to encourage behavior that is likely to result in cyber harassment. One website 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

---

145 Websites may take down material if they are served with a take down 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. For example, in a recent case, a plaintiff sued Autodesk because it sent an infringement notice to eBay, where the plaintiff was selling copies of Autodesk software products. 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. Vernor v. Autodesk, 555 F.Supp.2d 1164 (W.D. Wash 2008).

146 For example, Juicy Campus’s slogan was “C’Mon, Give us the Juice. Post are totally, 100% anonymous.” 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.
using those fake profiles.\(^{147}\) It encourages posters to submit “picks and videos to really tell the story!”\(^{148}\) These websites should be viewed as having made a calculated business decision to permit certain “high risk” activity on their websites and their liability should reflect that calculation. Website 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, website sponsors that have implemented policies to deal with cyber harassment, and that enforce such policies, should not be held liable for the conduct of their users.

The imposition of proprietorship liability upon website sponsors furthers the objectives of tort law. It deters antisocial conduct and compensates those injured by such conduct.\(^{149}\) It allocates the risk of injury to the party in the best position to avoid its occurrence and absorb the loss.\(^{150}\) The burden on the website sponsor in adopting a cyber 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.\(^{151}\)

Although the proposals introduced in Part IV contemplate voluntary adoption or self-regulation by website sponsors, they provide a standard by which to measure website sponsor conduct in determining tort liability. As proprietors, website sponsors should be required to take “reasonable measures” such as those set forth in Part IV to prevent tortious or criminal conduct on their websites. If the websites fail to have these or similar

\(^{147}\) See [www.gossipreport.com](http://www.gossipreport.com) (stating that “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!”)

\(^{148}\) Id.


\(^{150}\) Lawrence v. Bainbridge Apartments, 957 S.W.2d 400, 405 (Mo. Ct. App. 1997) (noting that tort law objective is to place the cost of the injury on the party in the best position to avoid the risk and absorb the loss).

\(^{151}\) This is an articulation of the formula famously stated by Learned Hand in *United States v. Carroll Towing Co.*, 159 F.2d 169 (2d Cir. 1947) as $B < PL$. 
policies and procedures in place to address cyber harassment or to curb its occurrence, or if they fail to enforce such policies, they should be found negligent for foreseeable harm caused by third parties. The adoption of the proposals introduced in Part IV or similar proposals may be viewed as the "reasonable measures" that website sponsors should take to protect their invitees from foreseeable third party harm.

The proposals in this Article will not banish all cyber harassment nor will it stop the most determined trolls; however, it does force website sponsors to recognize that there are measures they can take to curb abusive and damaging conduct on their websites. Cyber harassment is just too easy on the Internet. Perhaps most importantly, these proposals recognize and treat cyber 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 in cyberspace 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 websites may have the effect of forestalling government intervention efforts which may be more sweeping and invasive than actions taken by website 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 cyber harassment case has generated much consternation among legal experts. Because there was insufficient evidence to bring charges under state criminal statutes, federal prosecutors brought the indictment under the Computer Fraud and Abuse Act. The indictment stated that the Act was violated when Drew violated MySpace’s terms of service. Several legal
scholars argued that the prosecution sets a dangerous precedent since few people actually read website terms of service.  

IV. PROPOSALS TO ADDRESS THE PROBLEM OF CYBER HARASSMENT

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 cyber 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 those victims of cyber harassment who lack the resources to pursue available remedies and/or wish to avoid further publicity.  

It often exacerbates rather than ameliorates the emotional trauma of having had personal details or images released to an audience of millions. The permenance of Internet distributions also makes rehabilitation much more difficult. One undergraduate stated that it was much more difficult to continue his new life as a college student.

---


153 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 cyber harassment. He also introduces remedies, such as alternative dispute resolution measures, that would limit the impact of instances of cyber harassment. While I agree with many of Solove’s proposals, my proposals focus more on prevention of cyber harassment through primarily non-legal measures.
student after he was identified by name as having appeared in a pornographic movie in a post on the Juicy Campus website. The post also linked to a Web site that showed him engaging in explicit acts with other men.\footnote{Richard Morgan, \textit{A Crash Course in Online Gossip}, N.Y. TIMES, Mar. 16, 2008.}

These proposals recognize that some forms of cyber harassment have the potential to cause more harm than others. They also take into account that at least some forms of cyber harassment have the potential for social value, including expressive value, whereas the expressive value of other forms of cyber harassment is non-existent or negligible. 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 cyber 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 that may for economic or social reasons lack other forum for communication, it also has serious drawbacks. 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 in causing online disinhibition.\footnote{Suler, \textit{supra} note 50 (noting that “anonymity works wonders for the disinhibition effect.”).} Anonymous users feels less vulnerable about being frank and don’t feel responsible for their online conduct.\footnote{\textit{Id.}} Finally, the notion of anonymity itself is misleading. In the vast majority of 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

\begin{footnotesize}
\footnote{Richard Morgan, \textit{A Crash Course in Online Gossip}, N.Y. TIMES, Mar. 16, 2008.}
\footnote{Suler, \textit{supra} note 50 (noting that “anonymity works wonders for the disinhibition effect.”).}
\footnote{\textit{Id.}}
\end{footnotesize}
user identification. In addition, the website sponsor often requires registration and knows the identity of a poster, even if other users do not. My 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 website sponsors. Because of the private regulatory nature of the Internet, website sponsors are in the best position to address the problem of cyber harassment. Paradoxically, website sponsors have borrowed the rhetoric of free speech as though they were public forums while taking full advantage of their sites as private businesses. As discussed in Section IV, website sponsors currently occupy a unique position that enables them to exercise the benefits of proprietorship without being held liable for the consequences of such proprietorship. As a matter of fairness and consistency, website sponsors should have a duty to take reasonable steps to prevent tortious and criminal conduct on their websites, at least in certain circumstances. These reasonable steps should include having a policy in place to deter cyber harassment which includes at least some of the proposals set forth in the following section.

157 See Nunziato, supra note 13, at 1116 (noting that the “vast majority of speech on the Internet today occurs within private places and spaces that are owned and regulated by private entities.”).

158 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_. at 1116.
A. Contractual and Architectural Constraints

One way that posters may be prompted to reconsider their postings may be by implementing contractual and architectural restraints, many of which already exist on commercial websites. As many scholars have explained, the way that choices are presented influences their selection or non-selection. Object design or architecture along with human foibles and limitations influence decisions and object use (or misuse). What the following contractual and architectural constraints that I propose in this section do is create structural barriers to speech without unreasonably restricting speech. In other words, they may serve in their modest way the purposes that time, place and manner restrictions and physical, logistical and normative barriers imposed upon speakers in the physical world.

1. Manifesting Assent to Website Policies.

Website sponsors can require posters to register with the website prior to posting comments. Although posters can easily create email addresses and use false information, having to go through the motions of doing so may slow down the posting process or cause them to reconsider. As part of the posting process, a poster may be reminded of the

159 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 website’s terms of service against a minor. See A.V. v. iParadigms, LLC http://www.iparadigms.com/iParadigms_03-11-08_Opinion.pdf (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 which retaining their contractual benefits).
160 DONALD A. NORMAN, THE DESIGN OF EVERYDAY THINGS (1988) (discussing the influence of product design upon consumer behavior and use); RICHARD H. THALER & CASS R. SUNSTEIN, NUDGE (2008) (citing social studies to explain how choice architecture can be used to improve decision making); KIM VICENTE, THE HUMAN FACTOR (2006) (discussing how technological advancements must be designed with human limitations in mind).
website’s policy against cyber harassment. 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 its agreement. In the alternative, or in addition to expressing agreement to the terms of the website’s cyber 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 may also cause a poster to decide whether he or she really does want to continue. Website sponsors can also institute comments policies or moderate user comments.

2. **Indemnification for User Misconduct.**

Another possibly effective way for website sponsors to both discourage cyber harassment and protect themselves would be for website sponsors to require a user to contractually agree to indemnify them from any harm which results from the user’s actions. In Part III, I advocate the imposition of proprietorship tort liability upon website sponsors for foreseeable harm caused by third parties. Website sponsors, in turn, can reduce their risk of tort liability by contracting for indemnification with their users. In order to ensure enforceability, the agreement should be concise, understandable, and conspicuous. Furthermore, the user should be required to manifest assent by clicking, rather than burying the terms in a “terms of use” page. Requiring active assent may make the user realize that the website is serious about enforcing its cyber harassment policy and encourage the user to consider the legal repercussions of its actions.

3. **Community Controls.**

Of course, that would require that the website have such a policy.
In addition, the website might incorporate user generated controls on content. For example many websites such as YouTube enable users to click on a link to report offensive content or abusive conduct. Wikipedia enables users to update and delete content placed by others and has reportedly changed its policy so that new and anonymous users must have their content “flagged” or approved by registered, reliable users.\textsuperscript{162} eBay and Amazon enables users to rate other users. All of these controls can be incorporated on other websites as well. For example, a message board can have users rate the quality of a particular poster for the benefit of newcomers.\textsuperscript{163} The online version of the San Francisco Chronicle, for example, enables readers to click on an icon to indicate a “thumb’s up” or “thumb’s down” following a poster’s comments.\textsuperscript{164} Users can also report offensive posts and request such posters be banned from the website.

4. Default to Identified Postings.

Another architectural control that websites can implement is a default to identified rather than anonymous postings. Currently, much of Internet communication is structured to facilitate anonymous postings, and to accord each posting equal weight. Instead, communication can be structured to default to postings that identify the poster unless the poster opts to post anonymously by clicking out of the default \textit{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


\textsuperscript{163} Some news sites incorporate ratings systems where authorities evaluate news articles and are themselves rated. \textit{See} Cohen, \textit{supra} note 134.

required the user to click onto another page, rather than merely checking a box on the same page. Of course, there will continue to be posters who falsify their registration information and those who take the extra step to opt out of identification, but there may also be a few who do not. The point is not to make identified postings mandatory but, by making anonymous postings slightly more burdensome, to make identified postings the easier choice.

5. “Cooling Period.”

A website sponsor can incorporate certain hurdles or procedures to slow down the posting process, to allow 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 by requiring a “cooling period.” A poster might be required to wait a certain length of time before a message or image is posted to a website. 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 cyber harassment likely to occur on the website. 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 periods, or no waiting period at all, whereas anonymous posters may be subject to a lengthier cooling period. Any waiting period at

Notices may also deter misconduct. A notice may inform a poster of the legal consequences of his or her actions. Some posters may simply 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 top of mind 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. \(^{165}\) In that study, researchers created a MySpace page for “Dr. Meg” that identified her as a doctor. \(^{166}\) The researchers then found MySpace users who identified themselves as 18-20 years of age and who discussed sexual activity and substance use on their publicly viewable pages. \(^{167}\) “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


\(^{166}\) Id.

\(^{167}\) Id.
Three months later, the researchers learned that 42.1% of the MySpace pages had been changed compared to 29.5% in the control group.\textsuperscript{169}

In addition to notifying the poster of what constitutes potentially criminal and tortious activity, the poster should be informed of the website’s policies governing user activity, especially since many such policies restrict more types of activity than that 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. For example, MySpace endured much negative publicity in the wake of Lori Drew’s violation of the networking site’s prohibition against falsifying information.

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. Poster identities are usually known by the website sponsors and by internet service providers (“ISP”). Poster identity may be revealed where a lawsuit has been filed pursuant to a subpoena, even where the website and the poster wish to maintain anonymity. In some cases, website policies may permit unmasking users under certain conditions, a few of which I suggest in the next section. Informing posters of the tenuous nature of anonymity may cause some to modify their postings. To illustrate, it is unlikely that the law students who posted offensive comments about other law students on the AutoAdmit message board 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

\textsuperscript{168} Id.
\textsuperscript{169} Id. at 38.
might have declined to post at all given the damage to their reputations in the legal community.

In order to be most effective, these warnings and other notices should be in plain English so that they are comprehensible to most users. It may be helpful to include examples of what constitutes each type of prohibited conduct in the notices. Finally, the notices should appear at the time of posting, rather than as a general message on the website 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 the poster’s accountability for his or her actions. Anonymity encourages a lack of accountability because a poster may feel more comfortable posting a comment if his or her identity can remain hidden. There are valid arguments in favor of anonymity. Stripping all posters of anonymity to curb cyber harassment is an overbroad measure because it threatens to stifle many socially beneficial types of communication. Members of subcultures or minority social, racial, religious and/or political groups may fear repercussions for posting unpopular views or by expressing beliefs, desires or thoughts that do not conform to mainstream values or norms. An atheist may post responses that question God’s existence. A teenaged 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

---

170 See Robert Bartlett & Victoria C. Plaut, Blind Consent, (finding that shorter form click agreements in a more readable format appeared to make contract terms more salient and meaningful) (on file with author).
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. 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 cyber harassment, often of members of those very same minority or disempowered groups. Currently, the only way that a victim of cyber harassment can unmask the 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. One solution is to permit the victim of certain types of cyber harassment to unmask a harassing poster without filing a lawsuit.

i. Easy Unmasking of Anonymity

The “easy unmasking” of anonymity that I propose in this section is limited to situations where all of the following factors are present: the victim of the cyber

---

171 Christopher Wolf, Racists, Bigots and the Law on the Internet, ANTI-DEFAMATION LEAGUE, available at http://www.adl.org/Internet/Internet_law1.asp (explaining how the Internet is “a relatively cheap and highly effective way for hate 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”); Jessica Valenti, How the Web Became a Sexists’ Paradise, THE GUARDIAN, Apr. 6, 2007 (noting that on some online forums “anonymity combined with misogyny can make for an almost gang-rape like mentality”); “Democracy Gone Wild”: Hate Speech Infests Online Versions of Local Daily Newspapers, PASADENA WKLY., June 12, 2008. Andrew Chin observes 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.” Chin, supra note 65, at 310. Danielle Keats Citron provides an extensive discussion of how online anonymous mobs threaten the online speech of traditionally disadvantaged groups. See Citron, supra note 10.
harassment has been identified in a posting; the victim is a non-public 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 some victims of cyber 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 briefly discussed in Section I.

There are several reasons for permitting easy unmasking of a cyber harasser. 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 in cyberspace and permit the victim to imagine the
most terrible culprits. A female law student who was the target of cyber threats on the
law school admission message board, AutoAdmit, stated, “I…felt kind of scared because
it was someone in my community who was threatening physical and sexual violence and
I didn’t know who.” 172 In some instances, those fears are justified. In others, they may
not be. Enabling the victim of a cyber threat to put a face on his or her tormentor, helps
the victim determine what he or she should do next, whether it is filing a police report, or

172 Denis Cummings, Anonymous AutoAdmit Posters to Be Revealed in Court, FINDINGDULCINIA, Aug. 4,
AutoAdmit-Posters-to-be-Revealed-in-Court.html.
calling the harasser’s parents. The harasser may then feel social pressure to stop the
harassing behavior without legal intervention.

Some may argue that permitting the unmasking of the harasser subjects the
harasser to attacks by the victim. This is a legitimate concern; however, 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 and
so would not be applied 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 cyber gossip
pertained to a company or business entity, or where the individual was a public figure.173
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 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. While back biting and gossip exist
everywhere, in most cases the individual spreading the gossip must deal with the
consequences of doing so. He or she develops a reputation for reliability or
misinformation; he or she may also be sought out or shunned for the gossip. On the
Internet, however, credibility is detached from identity.174 The victim of cyber gossip

173 Of course, this would not foreclose the business or public figure’s ability to seek recourse under existing
legal remedies.
174 The chief executive of Digg, a news distribution site, argued that transparency and noting poster “red
flags” such as posting history, would be one way to control rumors on the Internet. Cohen, supra note 130.
may 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 cyber harassment. In some situations, such as where the victim and the cyber harasser occupy the same social milieu, such as attending the same school, 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. Easy unmasking would have allowed these female law students to socially shame their classmates, and would have made it more difficult for the posters to continue their messages unchecked.

Of course, an easy unmasking policy is unavailing where the poster is the website sponsor itself (such as an anonymous blogger) or where the poster has used an anonymity service. But it may reduce some instances of cyber harassment where the poster has a reputation that it wishes to preserve, or where they have the desire to post in a “truly anonymous” manner but not the know-how required in order to do so.

ii. Stigmatizing Anonymity

In order for easy unmasking to be effective, the website must have an effective registration process. Many websites require posters to register their email 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 and be “truly” anonymous. The website sponsor can deal with truly anonymous posters in one of several ways. It can ban truly anonymous posters from the website 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 searchability.

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. Website sponsors could also 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 forum. For example, the AutoAdmit posters used juvenile pseudonyms such as “playboytroll,” “Pauliewalnuts,” “Whamo” and “Spanky.”¹⁷⁵ Depriving these posters of such fanciful user names may reduce the online disinhibition effect. After having his identity revealed, “Whamo” claimed, “I didn’t mean to say anything bad….I said something really stupid on the…internet, I type for literally, like, 12 seconds, and it devastated my life.”¹⁷⁶

Finally, as previously suggested, the website 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.

¹⁷⁶ Margolick, supra note 1.
C. Notice and Take-Down of Certain Postings

Because of the volume of traffic on many websites, prescreening is impracticable. Given both the quantity of postings as well as the nature of posts (which are often subjective or difficult to verify), website sponsors are ill-equipped to determine the lawfulness of content even after it has come to their attention. Yet, in certain cases, to require website sponsors to take down certain posts upon request would not impose an undue burden upon them. This section argues that website 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 come 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 website should be required to remove the post upon request of the original poster. One alleged poster to a popular social networking website claimed that she posted information about her former partner that she later regretted. She claimed that the website refused to remove the post even after repeated requests. A failure to takedown the original post upon request should constitute unreasonable conduct. The website sponsor may be ill-positioned to verify the accuracy of posted content, but the poster may uncover additional information that makes the original post misleading or

177 Because this information was posted in the Comments section of another website, the author was unable to verify the veracity of the information, but see http://www.cheatingways.com/cheaters/dont-date-him-girl-the-lawsuit/.
false, or may have had time to reconsider what was originally posted. Unfortunately, the original poster is often unable to remove the post without the website sponsors cooperation. To require reasonable website sponsor conduct to include removal of content upon request of the poster does not require website sponsors to prescreen or to make subjective determinations of content accuracy. Furthermore, a website 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 & Minors).

Digital images and videos arguably have the potential to cause the greatest harm to victims of cyber harassment. Images tend to stick in the minds of their viewers. They may be harder to forget. The popular perception is that pictures don’t lie and that one picture is worth a thousand words.

The truth is, however, that images can distort the truth by presenting only part of the entire 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, however, publication of such images may have 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, there are two types of images that should be outright prohibited without written consent. The first category is images of minors. Images of minors should not be uploaded to publicly accessible websites without the written consent of their legal guardians. The second category is
images of nude people where the individual is identifiable from the image. 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 websites 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 website sponsor for at least one year after the digital image has been removed from the website. Unlike other user-supplied content, to require website sponsors to takedown these two types of images does not require them to make difficult subjective decisions regarding user-supplied content. Whether a person is nude is not difficult to determine. Determining whether a person is under 18 by looking at an image is more difficult, but the burden on the website sponsor is slight and the sponsor might simply take down the image upon request of the individual or guardian or ask for verification of the minor’s age.

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 website is not required to respond until after a takedown request has been made. In addition, many news publications and websites have already instituted a policy prohibiting publication of both types of images without consent, so the proposal simply mirrors the existing practice in the physical world (and the expectations of those individuals who live in it). The prohibition does not prevent the capturing of the image but 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 website without the consent of the children’s guardians.

V. CONSTITUTIONAL SCRUTINY OF PROPOSED ANTI-CYBER HARASSMENT POLICIES

Some website sponsors, viewing themselves as public forums for speech given the absence of such forums on the Internet, may wish to employ only those policies that would survive constitutional scrutiny.\(^{178}\) Some may view a court order that requires a website sponsor to take certain “reasonable steps” to be state regulation.\(^{179}\) Given that tort law “is really regulation in aid of the policy goals of compensation and deterrence,”\(^ {180}\) this observation is not offensive or surprising. Thus, some may argue that court mandated adoption of anti-cyber harassment strategies requires that these strategies be constitutional. While I find this argument weak,\(^ {181}\) I address it in this next section, where I explain how and why these strategies, with a few modifications, can survive constitutional scrutiny.

A. Contractual and Architectural Constraints are Content Neutral

---

\(^{178}\) To require website sponsors to take down content upon request of the poster does not appear to implicate First Amendment rights, especially where the website sponsor is not claiming status as a “publisher.”

\(^{179}\) Jack Balkin notes that where the government “creates incentives for private parties to censor each other,” there is “state action.” J.M. Balkin, Free Speech and Hostile Environments, 99 COLU. L. REV. 2295, 2296 (1999).


\(^{181}\) As the California Supreme Court noted in *Weirum v. RKO General*, 539 P.2d 36, 40 (Cal. 1975), “The issue here is civil accountability for the foreseeable results of a broadcast which created an undue risk of harm to decedent. The First Amendment does not sanction the infliction of physical injury merely because achieved by word, rather than act.”
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. While the effect may be to evaluate and filter speech, it is the poster, and not a government actor, that 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 restriction without violating free speech principles.\textsuperscript{182} It might, for instance, ban all postings during the hours of midnight and five in the morning on the theory that posters are more likely to engage in tortious or criminal behaviors during those hours.\textsuperscript{183} I do not advocate such a broad 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 website sponsors and users.\textsuperscript{184} My proposed contractual and architectural constraints, by contrast, merely encourage the exercise of best judgment and self-control.

B. \textit{Easy Unmasking Proposals Can Be Limited to Survive Constitutional Scrutiny.}

While 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

\begin{footnotesize}
\begin{enumerate}
\item[183] Sherbert v. Verner, 374 U.S. 398 (1963) (permitting governmental regulation of conduct protected by the free expression clause of the First Amendment if the conduct poses substantial threat to public safety, peace or order).
\item[184] Content neutral government regulations are subject to a less rigorous analysis than content-based regulations. \textit{See} Turner Broadcasting System, Inc. v. F.C.C., 520 U.S. 180 (1997).
\end{enumerate}
\end{footnotesize}
governmental interests against individual interests.\textsuperscript{185} The Supreme Court has never ruled on an absolute right to anonymity\textsuperscript{186} nor has it ruled on the issue of anonymous speech regarding non-public matters.\textsuperscript{187} In fact, language in the two Supreme Court cases recognizing a constitutionally protected right to anonymity suggests that it would not extend to false or fraudulent speech.\textsuperscript{188} Furthermore, while Internet anonymity has been recognized by lower courts,\textsuperscript{189} 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 cyber threats, cyber gossip and cyber confessionals, typically would not involve protected speech.\textsuperscript{190} Easy unmasking in these three situations is not likely to affect protected speech as they involve threats or defamatory statements. Even if the cyber gossip or confessionals involve events or facts that are true, they are invasive of privacy as they publicly disseminate private information about private individuals.

Finally, governmental regulations or court decisions may avoid any First Amendment challenges by making easy unmasking policies voluntary but encouraging their adoption.

\textsuperscript{185} Talley v. California, 362 U.S. 60 (1960) (striking down as unconstitutional a city ordinance prohibiting the distribution of handbills without identifying the sponsors); McIntyre v. Ohio Elections Commission, 514 U.S. 334 (1995) (holding that Ohio statute banning distribution of anonymous political campaign literature not justified by state interest in preventing fraud and libel and informing voters).

\textsuperscript{186} In Talley v. California, the city ordinance prohibited all anonymous leafleting. Talley, 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. McIntyre, 514 U.S. at 334.

\textsuperscript{187} The decision in Talley addressed an economic boycott; the decision in McIntyre dealt with political speech. Talley, 362 U.S. at 60; McIntyre, 514 U.S. at 334.

\textsuperscript{188} Talley, 362 U.S. at 538 (expressly noting that the Court was not deciding on ordinances limited to prevent fraud); 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).

\textsuperscript{189} See John Doe v. 2TheMart.com Inc., 140 F. Supp. 2d 1088 (W.D. Wash. 2001).

\textsuperscript{190} Of course, website sponsors could apply unmasking strategies to a wider range of conduct.
For example, the adoption of an unmasking policy may be evidence of reasonable care, but a failure to adopt such a policy would not constitute negligence.

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

There are anticipated objections to the outright prohibition on digital images of children and nude individuals. The first objection is that they limit the free speech of the poster. In many cases, digital images – at least of nudity -- would not be considered protected speech because they would be obscene or pornographic and within the government’s police power.\textsuperscript{191} The expressive nature is debatable as the poster is not the subject in the photograph; the act of expression then is the uploading of another’s image.\textsuperscript{192} 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, even where the subject is a public figure.

The government has a compelling state interest in protecting minors’ from abuse and exploitation – even where such abuse and exploitation comes from other minors. In fact, some Missouri lawmakers are considering an outright ban on sex offenders taking photographs of children primarily because of the ease with which such photographs can

\textsuperscript{191} See Heideman v. South Salt Lake City, 348 F. 3d 1182 (10th Cir. 2003) (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 businesses, including those not engaged in expressive activity). In fact, section 230 expressly does not apply to statutes criminalizing obscenity and child pornography. \textit{See} Section 230 (e).

\textsuperscript{192} Furthermore, nudity is not in and of itself expressive. \textit{See} City of Erie v. Pap’s A.M., 529 U.S. 277, 294 (2000).
be shared with other sex offenders on social networking sites.\textsuperscript{193} Georgia lawmakers have also considered a similar measure.\textsuperscript{194} Yet, recent studies indicate that cyber harassment of teens by their peers is a bigger threat than sexual predation online.\textsuperscript{195} Cyber harassment by peers includes not just images taken without the consent of the subject, but images taken by the subject him- or herself. As previously noted, the teenaged brain is still developing its empathy and long-range planning abilities,\textsuperscript{196} which may negatively affect some teens exploring their sexuality with the aid of technology. According to a recent study, 1 in 5 teenagers and 1 in 3 young adults are using cell phones and online technology to send or post nude or semi-nude images of themselves.\textsuperscript{197} 70\% of those who admitted to sending sexual images of themselves sent them to a boyfriend or a girlfriend. A teenager sending a sexy image to a significant other is not thinking that their relationship might meet an unpleasant end. In the aftermath of a break-up, teenagers and young adults aren’t 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. While young love doesn’t last forever, a digital image of

\textsuperscript{193}Keith Chrostowski, Missouri lawmakers ponder a ban on sex offenders photographing children, February 12, 2008, http://primebuzz.kcstar.com/?q=node/10022

\textsuperscript{194}Id.


\textsuperscript{196}See supra note 64.

\textsuperscript{197}SEX AND TECH: Results from a Survey of Teens and Young Adults, conducted by The National Campaign to Prevent Teen and Unwanted Pregnancy and Cosmogirl.com available at http://www.thenationalcampaign.org/sextech/PDF/SexTech_Summary.pdf.
one’s naked teen self might, haunting someone like a digital scarlet letter and limiting one’s future career choices and life opportunities. Women are more likely to be affected than men. Over 80% of survey respondents said that they thought the reason girls send sexy images is to get a guy’s attention (compared to 60% who thought guys did so to get a girl’s attention) and about 40% said they thought girls sent sexy images under pressure from a guy (compared to 18% who thought guys did so under pressure from a girl). News stories and court cases also indicate that young men are more likely to exact this type of revenge upon their ex-girlfriends.

The restriction on speech imposed by my 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 websites and would not preclude someone from posting photographs to an invitation-only, password-required, photosharing website. The restriction on speech (if in fact, these images would qualify as protected speech) applies only where the necessary consent is missing. Clear parameters could be established on response times or the number of requests required before determining that the website sponsor has acted unreasonably. A court could also require that a website could reasonably refuse notice-and-takedown requests unless they came from the person authorized to give such consent (i.e. from the parents or guardian of the minor or the adult subject of the nude image). Concerns that a website might be

---

198 Id.
199 For example, nude photos of Laure Manaudou, an Olympic swimmer from France, appeared on websites 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. See http://www.chicagotribune.com/sports/olympics/chi-laure-manaudou-080811-hl.0.6552632.story. Manaudou reported that, “(w)henever I typed Laure Manaudou on the Internet, it was horrible. I felt humiliated.” Id.
inundated with illegitimate requests might be tempered if requestors were fined for
failing to provide verification of their identities and standing to request the takedown.
Finally, the court might also conclude that reasonable conduct entails only taking down
images of nude non-public figures yet require images of nude public figures to contain
modesty coverings, such as those contained in offline publications.200

CONCLUSION

While there are admittedly difficulties in monitoring content, this should not mean
that websites should then have no obligation to deter or minimize cyber harassment on
their websites. Whether one concludes that websites are sui generis or “just like
property” is beside the point; website 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 that websites can take to deter cyber
harassment without having to pre-screen or make subjective decisions about user
supplied content. By suggesting actions that website sponsors can readily adopt, this
Article aims to shift the normative expectations of website sponsor behavior and to

200 Another 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 since 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 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.
reframe the problem of cyber harassment as one of a failure of business norms rather than of free speech gone wild.