September 2014

Combating Cyber-Victimization

Jacqueline D. Lipton
Case Western Reserve University School of Law, jdl14@case.edu

Combating Cyber-Victimization

Jacqueline D Lipton, Ph.D.[*]

Abstract

In today's interconnected society, high profile examples of online victimization abound. Cyber-bullies, stalkers and harassers launch attacks on the less powerful, causing a variety of harms. Recent scholarship has identified some of the more salient damage, including reputational harms, severe emotional distress, loss of employment, and physical assault. Extreme cases of online abuse have resulted in death through suicide or as a result of targeted attacks. This article makes two major contributions to the cyber-victimization literature. It proposes specific reforms to criminal and tort laws to address this conduct more effectively. Further, it situates those reforms within a new multi-modal regulatory framework. This new approach advocates a combination of enhanced public education initiatives, enhanced access to effective reputation management services, the development of more pro-bono reputation management strategies, reporting hotlines, social norms, and industry self-regulation. The goal is to combine law with other regulatory modalities in order to facilitate the development of a more civil and accountable global online society.

---

[*] Professor of Law and Associate Dean for Faculty Development and Research; Co-Director, Center for Law, Technology and the Arts; Associate Director, Frederick K Cox International Law Center, Case Western Reserve University School of Law, 11075 East Boulevard, Cleveland, OH, 44106, Email – JDL14@case.edu, tel – 216 368 3303. The author would like to thank Professor Lyrissa Barnett Lidsky, Professor Elizabeth Rowe, and Professor Ann Bartow for comments on an earlier draft of this article. Additionally, the author is extremely grateful for comments from participants at the 3rd Annual Privacy Law Scholars' Conference at the George Washington Law School, Washington D.C., June 3, 2010, including comments from Mr David Thompson, Professor Mary Fan, Professor Bruce Boyden, Professor Danielle Keats Citron, Mr Ryan Calo, Professor Jon Mills, Mr Avner Levin, Mr Doug Curling, Ms Eileen Ridley, Mr Stefaan Verhulst, and, Professor Joel Reidenberg. In particular, Professor Raphael Cohen-Almagor was extremely generous with his time and comments. All mistakes and omissions are, of course, my own.

Table of Contents

Introduction

"Once, reputation was hard-earned and carefully guarded. Today, your reputation can be created or destroyed in just a few clicks." [1]

Words can hurt. Whether true or false, whether spoken by friend or frenemy,[2] the cyber pen is mightier than the sword.[3] In today's networked society, abusive online conduct such as cyberbullying and cyber harassment can cause serious damage including severe emotional distress,[4] loss of employment,[5] and worryingly physical violence[6] or death.[7] Thirteen year

---

[1] MICHAEL FERTIK and DAVID THOMPSON, WILD WEST 2.0: HOW TO PROTECT AND RESTORE YOUR ONLINE REPUTATION ON THE UNTAMED SOCIAL FRONTIER, 2 (2010).

[2] "Frenemy" has been defined as "a person who pretends to be a friend but is actually an enemy; a rival with which one maintains friendly relations" (see http://dictionary.reference.com/browse/frenemy, last viewed on June 6, 2010).

[3] Raphael Cohen-Almagor, *Responsibility of Net Users* in MARK FACKLER and ROBERT S. FORTNER (eds), ETHICS, GLOBAL COMMUNICATION AND MEDIA, 11 (forthcoming, 2010) (page refs to draft proofs) ("Words can wound. Words can hurt. Words can move people to action.").

[4] See, for example, Jacqueline Lipton, *"We, the Paparazzi": Developing a Privacy Paradigm for Digital Video*, 95 IOWA LAW REVIEW 919 , 921-922 (2010) ("[Consider the fate of "Star Wars Kid",] a Canadian teenager who filmed himself playing with a golf ball retriever as if it was a light-saber from the *Star Wars* movies…. His video was posted to the Internet without his authorization. A variety of amateur video enthusiasts then adopted it on services such as YouTube. They created many popular, but extremely humiliating, mash-up videos of the youth. The young man ended up dropping out of school. He also required psychiatric care, including a period of institutionalization at a children's psychiatric facility.") [hereinafter, *We, the Paparazzi*]

[5] Danielle Keats Citron, *Cyber Civil Rights*, 89 BOSTON UNIVERSITY LAW REVIEW 61, 64 (2009) ("Victims who stop blogging or writing under their own names lose the chance to build robust online reputations that could generate online and offline career opportunities.") [hereinafter, *Cyber Civil Rights*].

[6] See, for example, BBC News, *Cyber Bullies Target Girl*, May 24, 2003, full text available at http://news.bbc.co.uk/2/hi/uk_news/england/nottinghamshire/2933894.stm, last viewed on March 16, 2010 ("[The victim's] family says there has been a two-year campaign of intimidation and she has twice been attacked in school."); Kara Carnley-Murrhee, *Cyberbulling: Hot Air or Harmful Speech? Legislation Grapples With Preventing Cyberbullying Without Squelching Students' Free Speech*, UF LAW, 17, 18 (Winter 2010) (describing case of 13 year old Hope Witsell who committed suicide after being the victim of a "sexting" campaign – a variation of cyberbullying in which sexually explicit images of the victim or sexually explicit messages about the victim are disseminated over digital communications services) [hereinafter, *Hot Air*]; Danielle Keats Citron, *Law's Expressive Value in Combatting Cyber Gender Harassment*, 108 MICHIGAN LAW REVIEW 373, 396-397 (2009) ("The online abuse inflicts significant economic, emotional, and physical harm on women in much the same way that work-place sexual harassment does.") [hereinafter, *Law's Expressive Value*]

[7] Danielle Keats Citron, *Mainstreaming Privacy Torts*, 98 CALIFORNIA L REV ___, [14] (forthcoming, 2010) ("Today, the physical harm associated with information

old Megan Meier who believed she had found a soul mate in the fictional "Josh Evans" on MySpace was driven to suicide by his spurning words.[8] This is but one of an increasing number of examples of abusive online conduct.[9] One in four teenagers reportedly experience cyberbullying.[10] Sixty-five per cent of children know someone who has been the victim of cyberbullying.[11] A 2006 Pew Internet study found that one third of online teenagers had been victims of online harassment and that forty per cent of social network users have been cyberbullied.[12] Online abuses – cyberbullying, cyberstalking and cyberharassment – disproportionately

---

disclosures can involve murder.") [hereinafter, *Mainstreaming Privacy Torts*].

[8] Gordon Tokumatsu and Jonathan Lloyd, *MySpace Case: "You're the Kind of Boy a Girl Would Kill Herself Over*", Jan. 26, 2009, NBC LOS ANGELES, available at http://www.nbclosangeles.com/news/local-beat/Woman-Testifies-About-Final-Message-Sent-to-Teen.html, last viewed on March 15, 2010 (describing the last electronic message sent by Megan Meier, the teenage victim of an infamous online cyberbullying incident before she committed suicide by hanging herself in her closet). See also discussion of the incident in Cohen-Almagor, *supra* note 3, at 16-22; Lyrissa Barnett Lidsky, *Anonymity in Cyberspace: What Can We Learn from John Doe?*, 50 BOSTON COLLEGE L REV 1373, 1385-6 (2009) (describing the Megan Meier incident and legal responses to it) [hereinafter, *John Doe*].

[9] For more examples of cyberbullying conduct involving school age children, see http://www.slais.ubc.ca/courses/libr500/04-05-wt2/www/D_Jackson/examples.htm, last viewed on March 16, 2010; see also Citron, *Mainstreaming Privacy Torts*, *supra* note 7, at [10-11] (giving examples of high profile cases of online abuses).

[10] Cohen-Almagor, *supra* note 3, at 22.

[11] *id*., at 23.

[12] *id.*

affect traditionally subordinated groups,[13] notably women,[14] children,[15] and minorities.[16]

The prevalence of this conduct suggests that more effective means are necessary to redress online wrongs and to protect victims' reputations. Action against cyber-abusers has posed significant challenges for the legal system. Because of the global and largely anonymous nature of the Internet, reliance on the law will always be time-consuming and expensive for victims. In the United States, many potential legal solutions will also face First Amendment hurdles.

Unlike previous writing in this area, this article situates the law in a broader regulatory context. The author makes specific suggestions for reform of tort and criminal laws, but more importantly places the legal debate into a larger multi-modal framework for protecting online reputations. This new framework combines specific legal reforms with extra-legal regulatory approaches, many of which will prove more affordable and effective for victims of online wrongs. Part I explores the categories of abusive online conduct that require regulatory attention: cyberbullying, cyber harassment and cyberstalking. These categories are contrasted with their offline counterparts. Part II identifies gaps in the current law as applied to abusive online conduct. It focuses on criminal law, tort law, and to some extent civil rights law. It suggests ways in which current laws could be updated to more effectively combat online wrongs.

---

[13] Citron, *Cyber Civil Rights*, *supra* note 5, at 65-66 (citing statistics from 2006 evidencing that cyber harassment is concentrated on women and to some extent also people of color, religious minorities, gays, and lesbians).

[14] Ann Bartow, *Internet Defamation as Profit Center: The Monetization of Online Harassment,* 32 HARVARD J L & GENDER 383, 392 (2009) ("As women gain visibility in the blogosphere, they are the targets of sexual harassment and threats. Men are harassed too, and lack of civility is an abiding problem on the Web. But women, who make up about half the online community, are singled out in more starkly sexually threatening terms – a trend that was first evident in chat rooms in the early 1990s and is now moving to the blogosphere …."); 394 ("Self-identifying as a woman online can substantially increase the risk of Internet harassment."); but note that some victims of online harassment are men: Citron, *Mainstreaming Privacy Torts*, *supra* note 7, at [14-15] (describing physical assaults and murders of abortion doctors where website list of abortion doctors was involved in identifying them); Citron, *Law's Expressive Value, supra* note 6, at 378 ("While cyber attackers target men, more often their victims are female.").

[15] Citron, *Law's Expressive Value*, *supra* note 6, at 398 (noting that younger individuals are particularly impacted by online abuses because their lives are "inextricably tied to the net").

[16] Citron, *Cyber Civil Rights*, *supra* note 5, at 65-66.

Part III proposes extra-legal regulatory mechanisms that might better protect individual reputations online. It surveys currently available options, such as commercial reputation management services,[17] along with their shortcomings. It advocates developing educational programs to empower victims of online abuses to utilize currently available legal and technological means for protecting their online reputations. It also suggests an increased role for reporting hotlines, evolving social norms, and industry self-regulation through codes of conduct and "naming and shaming" programs.

Part IV concludes by suggesting future directions in the regulation of online abuses. The advantages of developing these extra-legal approaches relate to easing the time and cost burdens on victims and avoiding some of the First Amendment concerns raised by legislated solutions. Additionally, development of these extra-legal avenues will ultimately change the climate of online discourse and facilitate a more civil and accountable global online society where service providers play a more active role in monitoring and enforcing norms of accountability.

I. Categorizing Abusive Online Conduct

A. Delineating the Boundaries of Online Abuses

1. Defining Online Abuses

> *"The Internet has turned reputation on its head. What was once private is now public. What was once local is now global. What was once fleeting is now permanent. And what was once trustworthy is now unreliable."* [18]

Recent literature describes online abuse predominantly in terms of cyberstalking, cyber harassment, and cyberbullying. None of these terms has achieved a universally accepted definition, and there are significant areas of overlap between them. Some authors have coined umbrella terms such cyber victimization[19] and cyber targeting[20] to encompass all of these

---

[17] See, for example, http://www.reputationdefender.com/, last viewed on April 14, 2010; http://www.youdiligence.com, last viewed on May 20, 2010; http://www.udiligence.com, last viewed on May 20, 2010; http://www.reputationhawk.com, last viewed on June 6, 2010.

[18] FERTIK and THOMPSON, *supra* note 1, at 44.

[19] Kate E Schwartz, *Criminal Liability for Internet Culprits: The Need for Updated State Laws Covering the Full Spectrum of Cyber Victimization*, 87 WASH U L REV 407 (2009).

[20] David A Myers, *Defamation and the Quiescent Anarchy of the Internet: A Case*

categories of conduct. These commentators have avoided individual terms for different cyber wrongs on the basis that overlaps between the classes of wrong might "thwart clear analysis and the creation of successful solutions".[21] There is some merit to the view that an umbrella term – such as online abuses, cyber abuses or cyber wrongs - is more effective than categorizing individual sub-classes of conduct, although there will be some circumstances in which the individual classifications are important.[22]

Nevertheless, a brief consideration of the kinds of conduct described in recent years as cyberbullying, cyber harassment and cyberstalking is useful background. These terms are derived from their offline counterparts – bullying, harassment, and stalking. As much current law, particularly state criminal law, is focused specifically on bullying, harassment, and stalking, it is necessary to understand the terms in order to appreciate the gaps in the current legal system.

2. Cyberbullying

> *"Bullying is an attempt to raise oneself up by directly demeaning others; the attacker hopes to improve his social status or self-esteem by putting others down."*[23]

The term cyberbullying generally refers to online abuses involving juveniles or students.[24] While it is possible that in any given instance of cyberbullying, at least one of the parties may not be a youth,[25] discussions

---

Study of Cyber Targeting, 110 PENN ST L REV 667 (2006).

[21] Schwartz, *supra* note 19, at 409.

[22] For example, as the following discussion demonstrates, cyber-harassment laws usually require a credible threat of immediate physical harm to a victim and thus are less likely to be successfully challenged under the First Amendment because threats are generally not protected speech: *Planned Parenthood of the Columbia/Willamette Inc v American Coalition of Life Activists*, 23 F. Supp. 2d 1182 (D. OR 1999) (threatening speech not protected by the First Amendment). See also discussion in Cohen-Almagor, *supra* note 3, at 5.

[23] FERTIK and THOMPSON, *supra* note 1, at 105.

[24] Schwartz, *supra* note 19, at 410-411 ("the term cyberbullying is typically used in reference to juveniles or students, but it is unclear exactly which party must be a minor for the situation at issue to constitute cyberbullying. Some commentators consider cyberbullying to be the internet counterpart to traditional playground bullying, which presupposes that the culprit and the victim are both minors. For others, the term is used to reference 'the victimization of minors,' regardless of whether the culprit is himself a minor or an adult. A third definition for cyberbullying requires that the culprit be a minor, but leaves open the possibility that the victim could be an adult, such as a teacher.")

[25] See, for example, Tokumatsu and Lloyd, *supra* note 8 (bully was mother of a school mate of 13 year old victim of cyberbullying).

about cyberbullying generally revolve around school-age children and often call on schools to address the issue.[26] The term bullying in the physical world has tended to describe conduct that occurs "when someone takes repeated action in order to control another person".[27] It can involve tormenting, threatening, harassing, humiliating, embarrassing, or otherwise targeting a victim.[28]

In recent years, the term has also been increasingly used in the employment context to describe hostile or threatening conduct in the workplace.[29] In this context, bullying is differentiated from other offensive conduct, such as harassment, on the basis that bullying tends to be targeted at a particular person for reasons other than the person's gender or race – the typical focus of harassment laws.[30] Targets of workplace bullying are

---

[26] See, for example, Cal Education Code § 32261(d) ("It is the intent of the Legislature in enacting this chapter to encourage school districts, county offices of education, law enforcement agencies, and agencies serving youth to develop and implement interagency strategies, in-service training programs, and activities that will improve school attendance and reduce school crime and violence, including vandalism, drug and alcohol abuse, gang membership, gang violence, hate crimes, *bullying, including bullying committed personally or by means of an electronic act*, teen relationship violence, and discrimination and harassment, including, but not limited to, sexual harassment.")(emphasis added); Andrew M Henderson, *High-Tech Words Do Hurt: A Modern Makeover Expands Missouri's Harassment Law to Include Electronic Communications*, 74 MO. L REV 379, 381 (2009) (" 'Cyberbullying is when a child, preteen or teen is tormented, threatened, harassed, humiliated, embarrassed or otherwise targeted by another child, preteen or teen using the Internet, interactive and digital technologies, or mobile phones.' While typical cases of cyberbullying focus on young people, adults can also be involved in such behavior."); Citron, *Law's Expressive Value*, *supra* note 6, at 410 ("parents and educators have an important responsibility to teach the young about cyber harassment's harms because the longer we trivialize cyber gender harassment, the more difficult it will become to eradicate it.")

[27] Henderson, *supra* note 26, at 381.

[28] *id.*

[29] ABC News Story, *Bullies in the Office: Bullying Worse than Sexual Harassment*, available at abcnews.go.com/index/playerindex?id=4527601 (last viewed on May 18, 2010); BullyOnline.Org, Bullying: What is It? ("Bullying is persistent unwelcome behaviour, mostly using unwarranted or invalid criticism, nit-picking, fault-finding, also exclusion, isolation, being singled out and treated differently, being shouted at, humiliated, excessive monitoring, having verbal and written warnings imposed, and much more. In the workplace, bullying usually focuses on distorted or fabricated allegations of underperformance."), available at http://www.bullyonline.org/workbully/bully.htm#Why, last viewed on May 20, 2010).

[30] Federal Communications Commission, *Understanding Workplace Harassment*, available at http://www.fcc.gov/owd/understanding-harassment.html, last viewed on May 20, 2010 (noting that harassment occurs in cases of "unwelcome verbal or physical conduct based on race, color, religion, sex (whether or not of a sexual nature and including same-gender harassment and gender identity harassment), national origin, age (40 and over), disability (mental or physical), sexual orientation…").

often perceived as a threat to the bully in some way.[31] This notion of bullying would cover the Megan Meier scenario where Lori Drew – the perpetrator of the "Josh Evans" scam – perceived Meier as a potential threat to her own daughter.[32] She targeted Meier because of this perceived threat, rather than because of Meier's gender or race, attributes that would be typically the subject of harassment law.

3. Cyber Harassment

Like harassment in the physical world, cyber harassment should technically focus on targeting people by virtue of their membership in a protected class: for example, race or gender.[33] There is a fine line between bullying and harassment, both online and offline. In cyberspace, as in the offline world, the distinctions between bullying and harassment tend to blur. Much conduct that has been described as cyber harassment involves mobbing behavior aimed at silencing women and racial minorities.[34] This conduct seems to cross the line between bullying and harassment. While it is directed at a protected class (women, racial minorities etc.), mobbing is typical of bullying[35] and the aim of driving subjugated groups offline seems more about control than possession – again, typical characteristics of

---

[31] BullyOnline.Org, *supra* note 29 ("Jealousy (of relationships and perceived exclusion therefrom) and envy (of talents, abilities, circumstances or possessions) are strong motivators of bullying.")

[32] Cohen-Almagor, *supra* note 3, at 19 (noting that Lori Drew had suggested talking to Megan Meier via the Internet to find out what Meier was saying online about Drew's daughter).

[33] Federal Communications Commission, *Understanding Workplace Harassment*, *supra* note 30.

[34] Citron, *Cyber Civil Rights*, *supra* note 5, at 64 ("[Noting] the growth of anonymous online mobs that attack women, people of color, religious minorities, gays, and lesbians. On social networking sites, blogs, and other Web 2.0 platforms, destructive groups publish lies and doctored photographs of vulnerable individuals. They threaten rape and other forms of physical violence. They post sensitive personal information for identity thieves to use. They send damaging statements about victims to employers and manipulate search engines to highlight those statements for business associates and clients to see. They flood websites with violent sexual pictures and shut down blogs with denial-of-service attacks. These assaults terrorize victims, destroy reputations, corrode privacy, and impair victims' ability to participate in online and offline society as equals. Some victims respond by shutting down their blogs and going offline. Others write under pseudonyms to conceal their gender, a reminder of nineteenth-century women writers George Sand and George Eliot. Victims who stop blogging or writing under their own names lose the chance to build robust online reputations that could generate online and offline career opportunities.")

[35] BullyOnline.Org, *supra* note 29 (describing "gang" or "group" bullying, also known as "mobbing").

bullying as opposed to harassment.[36]

Because of the overlaps between bullying and harassment and the fine distinctions between them, it may be appropriate – at least in the early days of online regulation – to address cyber-harms more universally and to worry about the distinctions later. In fact, new distinctions may emerge that are more appropriate in the digital age than some of the existing distinctions between classes of conduct. For example, regulators may choose to distinguish between communications specifically directed to an individual and general communications about an individual on the basis that the former conduct may be more immediately threatening or frightening to the victim. If direct communications contain threats, such conduct may be easier to regulate through legislation than general online communications directed to an audience at large. Where an immediate threat of harm is involved, speech is less likely to be protected by the First Amendment than general speech directed to the world at large.[37]

4. Cyberstalking

Cyberstalking is a good example of conduct directed to a victim rather than general communications about a victim. At least in some jurisdictions, cyberstalking legislation requires a credible threat to the victim.[38] Some commentators have described cyberstalking as a direct online analog to the offline crime of stalking. Cyberstalking may thus be defined as: "the use of the Internet, email, or other means of electronic communication to stalk or harass another individual".[39] Offline stalking has typically been defined as involving: "repeated harassing or threatening behavior".[40] The goal of the traditional stalker is to exert control over a

---

[36] Erica Merritt, *Workplace Bullying*, presentation at Case Western Reserve University, Cleveland OH, on May 18 ,2010 (session notes and PowerPoint slides on file with the author).

[37] See note 22, *supra*.

[38] Schwartz, *supra* note 19, at 411 ("one commentator states that cyberstalking is distinct from cyberbullying because cyberstalking involves credible threats").

[39] Naomi Harlin Goodno, *Cyberstalking, a New Crime: Evaluating the Effectiveness of Current State and Federal Laws*, 72 MO. L REV 125, 126 (2007); see also Shonah Jefferson and Richard Shafritz, *A Survey of Cyberstalking Legislation*, 32 U. WEST L.A. L REV 323, 323 (2001) ("cyberstalking is not easy to define, and no universal definition is accepted. One possible definition is 'the use of the Internet, e-mail [sic] or other electronic device to hound another person. It can involve ongoing harassment or threatening behaviour.' Query whether this definition really rises to the level of cyberstalking. Is hounding enough?")

[40] Goodno, *supra* note 39, at 127 ("Generally, the goal of a stalker is to exert 'control' over the victim by instilling fear in her; and often such conduct leads to physical

victim by instilling fear into her.[41] In the physical world, as in cyberspace, stalking can lead to actual physical harm.[42]

While cyberbullying and cyber harassment may damage an individual's reputation or livelihood, cyberstalking is more likely to result in severe and immediate emotional or physical harm. Thus, at the very least, legislation aimed at redressing cyberstalking may be able to stand up to First Amendment scrutiny more easily than legislation aimed at other kinds of online abuses.[43] While the First Amendment may protect my ability to say something unpleasant about you online – subject to defamation and privacy law – it is much less likely to protect my ability to send you threatening email messages.

B. Comparing Online and Offline Abuses

"[T]hanks to the power of the Internet, attackers and gossipmongers enjoy instant global audiences and powerful anonymity." [44]

Laws targeted at real world activities often do not translate well to cyberspace. Despite facial similarities between physical abuses and cyber-abuses,[45] there are significant underlying differences. Cyber-attackers can utilize the Internet to harass their victims on a scale never before possible both because of the immediate effect of their conduct and the global dissemination of online information.[46] This immediate and global dissemination is inexpensive for the abuser and is not particularly time-consuming.[47] Online postings have a *constant* effect on the victim, as opposed to more transient conduct in the physical world.[48] Even where

---

action.")

[41] *id.*

[42] *id.*, at 128 ("cyberstalking involves repeated harassing or threatening behavior, which is often a prelude to more serious behavior"); Citron, *Mainstreaming Privacy Torts*, *supra* note 7, at [14] (describing case in which online stalked led to murder of the victim by the stalker).

[43] See note 20, *supra*.

[44] FERTIK and THOMPSON, *supra* note 1, at 6.

[45] Goodno, *supra* note 39, at 128 ("Some experts believe that cyberstalking is synonymous with traditional offline stalking because of the similarities in content and intent. Similarities that are pointed to include: a desire to exert control over the victim; and, much like offline stalking, cyberstalking involves repeated harassing or threatening behavior, which is often a prelude to more serious behavior.")

[46] *id*., at 128-9.

[47] *id.*, at 129.

[48] *id*; Citron, *Mainstreaming Privacy Torts*, *supra* note 7, at [9] ("Emotional and reputational harm are alive and well today. In many ways, however, they are far worse.

information about a victim is removed from one website, it may be cached and copied on other websites.[49] Online communications have a permanent quality that real world conduct lacks.[50] Compounding the permanence effect is the fact that online information is easily searchable through Google and other popular search engines.[51] Thus, damaging information is more readily accessible to those who may be looking for it.

A cyber-attacker can also be physically removed from the victim. He may be across the state, across the country or across the globe from the victim.[52] The unlimited reach of the Internet differentiates online abuse from its offline counterparts in three important respects.[53] First, online abusers can act cheaply and easily from anywhere in the world.[54] Second, there is a sinister element in the secrecy of the attacker's location. The victim is constantly left wondering whether the attacker is in the next house or far away. [55] Finally, the global reach of the Internet leads to jurisdictional problems in enforcing laws against wrongdoers both in terms of law enforcement and in terms of gathering evidence from multiple jurisdictions.[56]

One might argue that online abuses are actually less serious than their offline analogs because the victim has the option of simply turning off the

---

While public disclosures of the past were eventually forgotten, memory decay has largely disappeared. Because search engines reproduce information cached online, people cannot depend upon time's passage to alleviate reputational and emotional damage.")

[49] *id*; Lipton, *We, the Paparazzi*, *supra* note 4, at 977 ("with projects such as the Internet Archive, many images will continue to be available in some form even after all 'live' images have been removed from relevant websites."); FERTIK and THOMPSON, *supra* note 1, at 54-55 (discussing the impact of the Internet Archive on the permanent quality of online information).

[50] *id*.

[51] FERTIK and THOMPSON, *supra* note 1, at 53-54 ("Conversations among friends were once conducted in private; they left no permanent trace once the last echo faded, and they could be spread only at the speed of interpersonal communication. Classroom notes were passed and trashed or at worst intercepted by a teacher and read aloud before being recycled. But many of those same conversations are now conducted online in a blog or chat room, in full view of the world, automatically indexed by Google, and broadcast to an audience of millions.")

[52] Goodno, *supra* note 39, at 129 ("Cyberstalkers can be physically far removed from their victim."); FERTIK and THOMPSON, *supra* note 1, at 61-62 ("Online, it is often impossible to know if the person you're chatting with is half a block or half a world away. The owner of a website might be your neighbor, or it might be someone in Azerbaijan.")

[53] Schwartz, *supra* note 19, at 129-130.

[54] *id*., at 129.

[55] *id*.

[56] *id.*, at 129-130.

computer and walking away. However, in today's interconnected world that is not a viable option. People who are forced offline forego important personal and professional opportunities.[57] Also, a victim moving offline herself does not stop others from posting harmful things about her that may continue to harm her personal and professional development despite her own choice not to read the postings. In many ways, it is better for a victim to know what is being said about her so she can take steps to combat the abuses. The question addressed in this article is how best to enable victims to combat harms and protect their own reputations.

The anonymity of online abusers also distinguishes them from their offline counterparts. While one might assume that online conduct is less harmful than the offline equivalent because it does not involve immediate physical contact, the opposite may be true.[58] The anonymity provided by the Internet may increase the volume of abusive conduct because it may encourage individuals who would not engage in such conduct offline to do so in the anonymous virtual forum provided by the Internet.[59] People are less inhibited when faced with a computer terminal than when faced with a real live person.[60] Cyberspace also enables perpetrators of online abuses to

---

[57] Citron, *Law's Expressive Value*, *supra* note 6, at 398 ("Although targeted women close their blogs, disengage from online communities and assume pseudonyms, they incur serious costs in doing so. Women miss opportunities to advance their professional reputations through blogging. They cannot network effectively online if they assume pseudonyms to deflect cyber abuse. They may lose advertising income upon closing their websites or blogs. Unless women are willing to forgo the internet's economic, social, and political opportunities, they cannot walk away from our networked environment without paying a high price."); Mary Madden and Aaron Smith, Pew Internet & American Life Project: Reputation Management and Social Media: How People Monitor Their Identity and Search for Others Online (May 26, 2010), 3 ("12% of employed adults say they need to market themselves online as part of their job.")

[58] Schwartz, *supra* note 19, at 130.

[59] *id*.

[60] *id*., at 130-131 ("The environment of cyberspace allows individuals to overcome personal inhibitions. The ability to send anonymous harassing or threatening communications allows a perpetrator to overcome any hesitation, unwillingness, or inabilities he may encounter when confronting a victim in person. Perpetrators may even be encouraged to continue these acts."); Cohen-Almagor, *supra* note 3, at 10 ("The Internet has a dis-inhibition effect. The freedom allows language one would dread to use in real life, words one need not abide by, imagination that trumps conventional norms and standards."); Lidsky, *John Doe*, *supra* note 8, at 1383 ("Anonymity frees speakers from inhibitions both good and bad. Anonymity makes public discussion more uninhibited, robust, and wide-open than ever before, but it also opens the door to more trivial, abusive, libelous, and fraudulent speech.") ; Lyrissa Barnett Lidsky and Thomas Cotter, *Authorship, Audiences, and Anonymous Speech*, 82 NOTRE DAME L REV 1537, 1575 (2007) ("Studies show that even when an Internet user is *not* anonymous and knows the recipient of his e-mail message, the speaker is more likely to be disinhibited when engaged in 'computer

spy on their victims in virtual space for extended periods of time without ever being detected.[61] And naturally anonymity makes it more difficult for victims and law enforcement officers to identify and locate cyber-wrongdoers.[62]

Another unique feature of cyberspace is that it enables perpetrators to manipulate the victim's identity online.[63] Cyber-abusers can both impersonate their victims and can manipulate others' reactions to their victims.[64] Wrongdoers may engage in identity theft for financial purposes.[65] Additionally, they may pretend to be their victims, and send inflammatory messages to online discussion groups or social networks in the guise of the victim suggesting, for example, that the victim has fantasies of being raped.[66] Retaliation against the victim often follows. Retaliation might include the victim being banned from certain websites, being threatened by those who perceive her conduct as inappropriate, or being propositioned by people who have been misled into thinking that she is interested in engaging in unorthodox sexual activities.[67]

---

mediated communication' than in other types of communications. The technology separates the speaker from the immediate consequences of her speech, perhaps (falsely) lulling her to believe that there will be no consequences. Since the Internet magnifies the number of anonymous speakers, it also magnifies the likelihood of false and abusive speech."); FERTIK and THOMPSON, *supra* note 1, at 76-78 (describing psychological studies on disinhibition effects when perpetrators of harm are physically removed from their victims).

[61] Schwartz, *supra* note 19, at 131.

[62] *id*.

[63] FERTIK and THOMPSON, *supra* note 1, at 78-79 ("[T]he anonymity provided by the Internet allows attackers to easily impersonate others. On many sites, the lack of verifiable identity allows malicious (or mischievous) users to enter somebody else's name as their own…. Attacks by impersonation can be particularly harmful: How do you prove that you didn't really make an offensive comment that appears to be posted under your name? How do you show that it wasn't really you who engaged in a juvenile spat online?")

[64] Schwartz, *supra* note 19, at 131-133.

[65] Citron, *Mainstreaming Privacy Torts, supra* note 7, at [12] ("Data leaks lead to identity theft and fraud. Identity thieves use SSNs, biometric data, and insurance information to empty bank accounts, take out credit cards, secure loans, and flip property. They can destroy someone's credit, precluding their ability to borrow money. Identity theft can undermine individuals' ability to obtain employment as employers access individuals' credit reports in making hiring decisions. Some individuals can repair their credit reports but only after spending on average over $5,720. Others, however, may lack the knowledge and means to repair their credit reports. They may be unable to take out loans and get insurance. They might even face financial ruin. Medical identity thieves leave individuals with hefty hospital bills and someone else's treatment records.")

[66] *id*., at [15-16] (describing cases where cyber-abusers have posted false "rape fantasies" online in the names of targeted victims).

[67] *id*.

Thus, the conduct of a cyber-abuser may be differentiated from that of a physical world wrongdoer in that the online abuser does not necessarily communicate a direct threat to the victim. Instead, he can use general online communications not specifically directed to his victim in order to incite others to directly threaten or harm the victim. In many cases these puppet actors used by the original attacker will not even be aware that their activities are unwelcome or threatening in any way. This may occur where, for example, a puppet believes that the victim harbors rape fantasies and thinks he is merely playing out those fantasies rather than scaring or harming the victim. For example, in several cases involving the popular website Craigslist, bad actors posted messages giving personal details of intended victims, including their home addresses, and saying that the victims harbored rape fantasies.[68] In at least one case, the intended victim was actually raped by a third party who claimed he acted at the victim's invitation and that he was merely fulfilling what he thought was her rape fantasy.[69]

It is very difficult for victims of these kinds of impersonation attacks to effectively fight back in practice. Because identities are extremely difficult to verify online, it can be almost impossible for a victim to establish that she was not the person who posted the comments in question.[70] It is very difficult for the victim to prove a negative: that is, the "I didn't do it" part of the equation.[71] Even if she can, the victim's revocation may attract more attention to the original content and ultimately make the damage worse.[72] Additionally, even if the victim has a way of proving the negative, it may be extremely difficult for her to connect with the appropriate audience for her rebuttal of the perpetrator's conduct. Many websites – like blogs – will list comments in order of posting. Thus, a rebuttal by the victim may be deprioritized at the end of a comment list where few readers are likely to see it.[73] As noted by the founder and the general counsel of ReputationDefender, "many victims feel completely helpless when faced with an anonymous impersonator".[74]

---

[68] *id*., at [15]

[69] *id*.

[70] FERTIK and THOMPSON, *supra* note 1, at 79.

[71] *id.*

[72] *id*., at 144 ("Replying [to false-flag attacks] often draws more attention to the original content, making the damage worse.")

[73] *id* ("And a repudiation [of a false flag comment] might never be seen: because some websites list their comments in order by the date they were submitted, a late repudiation may show up far down the page and thus be practically invisible.")

[74] *id*.

II. Redressing Online Wrongs: Gaps in the Existing Legal Framework

A. Criminal Law

1. Criminal Law versus Civil Law

Current criminal laws, including those targeted specifically at online conduct, fail to comprehensively deal with today's cyber-abuses. Existing disharmonized state laws cannot effectively deter conduct that typically crosses state or national borders. Criminal law shares with civil law the shortcoming that victims are forced to relive the humiliation, embarrassment, shame, and fear attached to the defendant's conduct on the public judicial record.[75] Closed criminal trials may be preferable in particularly sensitive cases.[76] Absent effective privacy protections, victims of online abuses may be reticent to make complaints or to give evidence in court.

Unlike civil law, criminal law does not typically require a victim to shoulder the costs of a laywer or the associated costs of litigation. However, effective criminal law does require prosecutors and police to be sufficiently well versed in the law and in the online conduct to make a credible case against the abuser.[77] The current lack of reliable data on the prevalence of cyberstalking might be attributable to both the failure of victims to bring complaints, and the lack of adequate training and funding for police and prosecutors effectively to deal with online abuses.[78]

---

[75] Lipton, *We, the Paparazzi*, *supra* note 4, at 961 ("Plaintiffs are put in the awkward position of having to relive the humiliation and embarrassment of the images as they are entered into the public record as part of the court proceedings.")

[76] Closed criminal trials raise constitutionality concerns and have been difficult to achieve in practice in other contexts. See, for example *Press Enterprise Co v Superior Court*, 478 U.S. 1 (1986) (court reversed order sealing transcript of lower court proceedings on First Amendment grounds).

[77] Citron, *Law's Expressive Value*, *supra* note 6, at 402-3 ("[Police officers] are often either incapable of properly investigating harassment or unwilling to do so until it has traveled offline. Officers often advise victims to ignore the cyber harassment until that time."); FERTIK and THOMPSON, *supra* note 1, at 6 ("Law enforcement … lags behind the Internet. In the United States, online law enforcement has generally been focused on major fraud and child pornography. Many victims of 'routine' online attacks cannot obtain help from the legal system, either because the attackers have disappeared into the digital night or because local courts and lawyers simply don't know how to deal with complex online attacks that might have come from the far side of the world.")

[78] Goodno, *supra* note 39, at 156 ("The lack of data [about the prevalence of

Despite its shortcomings, criminal law may be a better option than civil law for redressing many online wrongs. Criminal law seeks to punish and deter wrongdoing while civil law seeks to provide remedies that make a plaintiff whole.[79] Where the concern is with deterring and punishing aberrant conduct, criminal law will be an important part of the regulatory matrix. Because of their importance to the regulatory matrix, criminal laws should be better harmonized and specifically targeted to today's most prevalent online abuses. The following examination of current state and federal criminal laws identifies existing gaps in these laws in the online context, and makes suggestions for law reform.

2. State Criminal Law

In recent years a number of states have enacted laws targeted specifically at online conduct.[80] However, most states still rely on pre-Internet legislation.[81] Nebraska, for example, maintains stalking and harassment legislation that does not expressly contemplate electronic conduct. The Nebraska Revised Code states that: "Any person who willfully harasses another person … with the intent to injure, terrify, threaten, or intimidate commits the offense of stalking."[82] In this context, "harassment" is defined as conduct: "directed at a specific person which seriously terrifies, threatens, or intimidates the person and which serves no legitimate purpose".[83] "Course of conduct" is defined as: "a pattern of conduct composed of a series of acts over a period of time, however short, evidencing a continuity of purpose, including a series of acts of following, detaining, restraining the personal liberty of, or stalking the person or telephoning, contacting, or otherwise communicating with the person".[84]

This legislative approach fails to cover a number of prominent

---

cyberstalking] is partly because many cyberstalking victims do not report the conduct to law enforcement, and partly because law enforcement agencies have not had adequate training in how to deal with it.")

[79] Schwartz, *supra* note 19, at 427 ("cyber-victimization is better suited to prosecution under criminal law, which seeks to punish and deter wrongdoing, than liability under civil law, which seeks to make a person whole.")

[80] Carnley-Murrhee*, Hot Air, supra* note 6, at 18 ("In the void of federal legislation, many states have enacted anti-cyberbullying laws. In the last decade, 19 states … have enacted laws that prohibit cyberbullying with state boundaries…").

[81] *id*.

[82] Neb. Rev. Stat. § 28-311.03 (2010).

[83] *id*., § 28-311.02(2)(a) (2010).

[84] *id*., § 28-311.02(2)(b) (2010).

online abuses. Online conduct will not amount to "detaining" or "restraining the personal liberty of" the victim. Online conduct may not even comprise "following" a person if the term "following" is confined to its traditional physical meaning. Stalking someone's online activities may not be the same as following a person in the physical world. Additionally, the statutory definition of "course of conduct" contemplates that the perpetrator must have directly targeted the victim. In its application to communications technologies, the statute requires a direct communication to the victim. This requirement does not fit the realities of cyber-victimization. Much online harassment involves the perpetrator posting online messages *about* the victim or even *in the guise of* the victim, rather than communications *directed to* the victim.

New Jersey previously maintained a stalking law similar to Nebraska's law. However, the New Jersey statute was updated in 2009. The current definition of "course of conduct" in New Jersey contemplates:

> "repeatedly maintaining a visual or physical proximity to a person; directly, indirectly, or through third parties, by any action, method, device, or means, following, monitoring, observing, surveilling, threatening, or communicating to or about, a person, …; repeatedly committing harassment against a person; or repeatedly conveying, or causing to be conveyed, verbal or written threats or threats conveyed by any other means of communication or threats implied by conduct or a combination thereof directed at or toward a person."[85]

Unlike Nebraska's law, the New Jersey statute contemplates activities utilizing *any kind of device* for monitoring, observing, surveilling, threatening, or communicating *to or about* a victim. This is a better model for legislation aimed at online conduct. It clearly covers electronic communications devices as well as online conduct that involves posting messages about a victim, rather than directed to the victim. Nevertheless, it is unclear even under this model whether a perpetrator who disguises himself as the victim and posts messages under the victim's name would be covered. Consider, for example, the scenario where a perpetrator uses the victim's identity to make online comments suggesting that the victim wants

---

[85] N.J. Stat. 2C: 12-10(a)(1) (2010)

to be raped and providing her personal contact details.[86]

It may be difficult for a prosecutor to convince a court that the perpetrator here is effectively "communicating about a person" for the purposes of the New Jersey statute. Where a perpetrator is pretending to *be* another person, he is in a sense communicating *about* that person because anything he does in the guise of the victim indirectly communicates his views – be they true or false – about the victim. However, this conduct is not the same as writing something about the victim in the third person. A court might hold that the legislative intent of the statute was limited to comments about the victim made by a person *other than the victim*, rather than comments made *in the guise of the victim*.

Even if the New Jersey statute is broad enough to cover incitement of third parties to harass the victim, many other state statutes – even relatively recent statutes aimed directly at online conduct – are not as broadly drafted as the New Jersey statute. For example, Florida's relatively new cyberstalking legislation defines cyberstalking as engaging: "in a course of conduct to communicate, or to cause to be communicated, words, images, or language by or through the use of electronic mail or electronic communication, directed at a specific person, causing substantial emotional distress to that person and serving no legitimate purpose."[87] Under this provision, there seems to be little doubt that a perpetrator posing as a victim online would not be communicating information *directed at a specific person*.[88] Thus, while the New Jersey statute may cover these kinds of scenarios, the Floridian statute will not extend this far. The differences in drafting between the criminal laws in different states also cause significant disharmonization concerns where abusive online conduct crosses state borders.

3. Federal Criminal Law

a. Interstate Communications Act

One solution to the problem of disharmonized state law would be

---

[86] Citron, *Mainstreaming Privacy Torts*, *supra* note 7, at [15-16].

[87] Fla. Stat. § 748.048(1)(d) (2009).

[88] See also Goodno, *supra* note 39, at 145 ("Although [the] group of state laws which overtly deal with cyberstalking is clearly a step in the right direction, these statutes have gaps …. Few of them explicitly address situations where the cyberstalker dupes an 'innocent' third party to harass."); 146 ("As of March 2007, only three states, Ohio, Rhode Island, and Washington, have statutes that explicitly address cases where third parties innocently harass the victim at the cyberstalker's bidding.")

greater focus on federal criminal legislation. Unfortunately, the current federal legislation contains many gaps and inconsistencies when applied to online abuses.[89] The federal laws that are most relevant to online wrongs are mainly found in those sections of the United States Code that deal with electronic communications and computer systems. The Interstate Communications Act, for example, provides that: "Whoever transmits in interstate or foreign commerce any communication containing any threat to kidnap any person or any threat to injure the person of another, shall be fined under this title or imprisoned not more than five years, or both."[90] This provision has limited application to online abuses because of its requirement of a threat of physical injury. [91] Many online abuses do not contain overt physical threats. In fact, many abusive communications are not specifically directed at their targets, but rather are comments *about* their targeted victims on generally accessible websites. [92] The Interstate Communications Act will also not cover situations where a perpetrator poses as a victim online to incite third parties to harass or harm the victim.

b. Telephone Harassment Act

The federal Telephone Harassment Act may have some application to online abuses. As amended in 2006, the statute prohibits a person from making a telephone call or utilizing a communications device without disclosing his identity and "with intent to annoy, abuse, threaten, or harass any person at the called number or who receives the communications".[93] The revisions to the statute were intended to capture harassing email messages.[94] While the provision will cover some cyberspace abuses, particularly the sending of threatening or harassing emails, it has significant limitations. For one thing, it is limited to acts "in interstate or foreign communications,"[95] although this may not be a very significant hurdle in practice. Courts may hold that any activities involving global communications devices – such as the Internet - occur in interstate or foreign communications.

More importantly, the statute will not cover situations where an Internet communication is not directed towards a particular recipient. The

---

[89] Carnley-Murrhee, *Hot Air, supra* note 6, at 18 (describing federal legislation in the cyberbullying area as being a "void").

[90] 18 U.S.C. § 875(c).

[91] Goodno, *supra* note 39, at 147-148.

[92] *id*.

[93] 47 U.S.C.S. § 223(a)(1)(C).

[94] Goodno, *supra* note 39, at 148-9.

[95] 27 U.S.C.S. § 223(a)(1).

requirement that the victim must be the recipient of a specific communication will not cover situations where a perpetrator simply posts information about the victim on a website, or where he poses as the victim.[96] Another limitation of the statute is that it carves out situations where the perpetrator has not remained anonymous.[97] In order for the prohibition to apply, the perpetrator must have failed to disclose his identity.[98] In cases where a victim knows the identity of the harasser, the statute will not apply.

c. Interstate Stalking Punishment and Prevention Act

Another recently amended federal statute that may apply to online abuses is the Federal Interstate Stalking Punishment and Prevention Act (FISPPA). This statute prohibits harassment and intimidation in "interstate or foreign commerce"[99] and now specifically extends to conduct that involves using "the mail, any interactive computer service, or any facility of interstate or foreign commerce to engage in a course of conduct that causes substantial emotional distress". As with the Telephone Harassment Act, the extent to which the "interstate or foreign commerce" requirement will limit the potential application of the FISPPA is unclear.

However, the FISPPA improves on the Telephone Harassment Act to the extent that it does not require a communication to be specifically directed to a victim. The FISPPA focuses instead on conduct that utilizes an interactive computer service to create a state of emotional distress in the victim, regardless of whether any communications posted on the computer service were specifically directed to the victim as a recipient.[100] Unlike the

---

[96] Goodno, *supra* note 39, at 150 ("[The Telephone Harassment Statute] applies only to direct communications between the stalker and victim, e.g., the statute would only be triggered when the cyberstalker sends an e-mail [sic] directly to the victim. Thus, the amended statute is inadequate to deal with behavior where the cyberstalker indirectly harasses or terrorizes his victim by posting messages on a bulletin board, creating a Website aimed at terrorizing his victim, or encouraging third parties to harass the victim.")

[97] *id*. ("It seems odd to only make cyberstalking a crime where the identity of the cyberstalker is unknown. This element seemingly, and without reason, carves out a number of terrifying cases where the victim knows the identity of the cyberstalker.")

[98] Lidsky and Cotter, *supra* note 60, at 1590 (raising constitutional concerns about the validity of this statute on First Amendment grounds because the statute fails to protect constitutionally protected values inherent in the defendant's anonymity).

[99] 18 U.S.C.S. §§ 2261A(1), 2261A(2).

[100] Goodno, *supra* note 39, at 152 ("[T]he newly amended § 2261A addresses many of the shortcomings of the other federal statutes. It does not have a 'true/credible threat' requirement; but rather adopts a standard that measures the victim's 'reasonable fear' or 'substantial emotional distress.' ")

Telephone Harassment Act, the FISPPA will apply where the defendant is not anonymous.[101] Like the other federal legislation described above, the FISPPA does not expressly deal with situations where the perpetrator of the online abuse poses as the victim online.

d. Computer Fraud and Abuse Act

One other federal criminal law that may be relevant to online abuse is the Computer Fraud and Abuse Act (CFAA).[102] This legislation was originally aimed at unauthorized hacking into computer systems and was not focused on personal attacks. However, prosecutors in the Megan Meier/Lori Drew case utilized the CFAA creatively to bring criminal proceedings against Drew, who had perpetrated a cyberbullying attack resulting in the suicide of thirteen year old Meier.[103] Drew was the mother of a classmate of Meier and knew that Meier struggled with depression. On the popular social networking site, MySpace, Drew posed as a sixteen year old boy named Josh Evans who started a friendship with Meier and later sent her insulting and harassing messages, concluding with a message that the world would be better off without her.[104] Evans never really existed. He was a fictional creation of Drew, who had developed the Evans persona to find out whether Meier would say anything negative about Drew's daughter online.[105]

Drew's conduct was not a criminal act under local Missouri law.[106] However, federal prosecutors charged Drew with unauthorized access to a computer under the CFAA. They utilized the criminal trespass provisions of the statute arguing that Drew had infringed MySpace's terms of service by failing to provide accurate registration information, engaging in abusive conduct, and harassing other people.[107] During the initial trial, a jury found that Drew had infringed provisions of the CFAA relating to making

---

[101] *id*. ("[The FISPPA does not] limit coverage of the 'use' of the computer to only anonymous e-mail [sic] messages.")

[102] 18 U.S.C. § 1030.

[103] Henderson, *supra* note 26, at 393 ("Despite her egregious actions, Missouri officials were unable to charge Lori Drew with a crime. However, after creatively interpreting the federal Computer Fraud and Abuse Act, federal officials charged her with conspiracy and unauthorized access of a computer."); Lidsky, *John Doe*, *supra* note 8, at 1386 (describing the legal action in the Lori Drew case).

[104] Henderson, *supra* note 26, at 379.

[105] *id*., at 379-380.

[106] *id*., at 380.

[107] *id*., at 393.

unauthorized access to, or exceeding authorized access to, a computer.[108] However, on appeal, a motion by Drew to acquit and overturn the misdemeanor conviction was upheld.[109] The court found that the CFAA would be void for vagueness if it imposed criminal liability on anyone who infringed a website's posted terms of service.[110] Thus, Drew's misuse of the MySpace website could not result in criminal liability under the CFAA.

e. Megan Meier Cyberbullying Prvention Bill

In the wake of the Meier incident, federal legislation was proposed that would be more clearly directed at cyberbullying than any existing federal laws. The Megan Meier Cyberbullying Prevention Bill[111] was introduced in 2008 but never enacted. If it had been implemented, it would have prohibited transmitting a communication "with the intent to coerce, intimidate, harass, or cause substantial emotional distress to a person" and "using electronic means to support severe, repeated, and hostile behavior".[112] The definitions of "communication" and "electronic means" in the bill were fairly broad and, if enacted, would have encompassed modern Web 2.0 technologies such as blogs and online social networks.[113]

While this legislation would have been broad enough to cover much abusive online conduct, it is arguably overbroad for a variety of reasons.

---

[108] *United States v Drew*, 259 F.R.D. 449, 453 (2009) ("The [trial] jury did find Defendant 'guilty' 'of [on the dates specified in the Indictment] accessing a computer involved in interstate or foreign communication without authorization or in excess of authorization to obtain information in violation of Title 18, United States Code, Section 1030(a)(2)(C) and (c)(2)(A), a misdemeanor.'")

[109] *United States v Drew*, 259 F.R.D. 449 (2009).

[110] *id*., at 464 ("The pivotal issue herein is whether basing a CFAA misdemeanor violation as per 18 U.S.C. §§ 1030(a)(2)(C) and 1030(c)(2)(A) upon the conscious violation of a website's terms of service runs afoul of the void-for-vagueness doctrine. This Court concludes that it does primarily because of the absence of minimal guidelines to govern law enforcement, but also because of actual notice deficiencies. ….[T]erms of service which are incorporated into a browsewrap or clickwrap agreement can, like any other type of contract, define the limits of authorized access as to a website and its concomitant computer/server(s). However, the question is whether individuals of 'common intelligence' are on notice that a breach of a terms of service contract can become a crime under the CFAA. Arguably, they are not."); 467 ("In sum, if any conscious breach of a website's terms of service is held to be sufficient by itself to constitute intentionally accessing a computer without authorization or in excess of authorization, the result will be that section 1030(a)(2)(C) becomes a law that affords too much discretion to the police and too little notice to citizens who wish to use the [Internet].'")

[111] H.R. 6123, 110th Cong. (2008).

[112] *id*. at § 3(a).

[113] *id*., at § 3(a).

For one thing, it is not confined to a repeated course of conduct and so could inadvertently catch one-time situations where people have acted uncharacteristically out of anger in the heat of the moment.[114] Additionally, while aimed at the Meier incident and drafted with a view to protecting minors,[115] the text of the statute is not expressly limited to conduct involving minors. As a result, the bill may be unconstitutional on First Amendment grounds because it may inadvertently sanction constitutionally protected expression amongst adults.[116]

In the wake of the Meier incident, the Missouri legislature updated the state harassment law to ensure that online bullying would be covered. As now drafted, the Missouri anti-harassment law provides that:

> "A person commits the crime of harassment if he or she:
>
> ….
>
> (3) Knowingly frightens, intimidates, or causes emotional distress to another person by anonymously making a telephone call or any electronic communication; or
>
> (4) Knowingly communicates with another person who is, or who purports to be, seventeen years of age or younger and in so doing and without good cause recklessly frightens, intimidates, or causes emotional distress to such other person; or
>
> …
>
> (6) Without good cause engages in any other act with the purpose to frighten, intimidate, or cause emotional distress to

---

[114] ROBERT SUTTON, THE NO ASSHOLE RULE: BUILDING A CIVILIZED WORKPLACE AND SURVIVING ONE THAT ISN'T, 11 (2007) ("Psychologists make the distinction between states (fleeting feelings, thoughts, and actions) and traits (enduring personality characteristics) by looking for consistency across places and times…").

[115] H.R. 6123, 110th Cong., § 2 (2008) (contemplating that the purpose of the bill is to protect children aged from 2 to 17 years old).

[116] In the past, legislatures have had difficulty establishing that laws abridging online speech are sufficiently narrowly tailored to survive First Amendment scrutiny. See, for example, *Reno v American Civil Liberties Union*, 521 I.S. 844 (1997) (holding that a statute attempting to restrict minors' access to harmful material was unconstitutional under the First Amendment); *Ashcroft v American Civil Liberties Union*, 542 U.S. 656 (2004) (holding that a statute that imposed criminal penalties for posting content harmful to minors on the Internet was unconstitutional under the First Amendment).

> another person, cause such person to be frightened, intimidated, or emotionally distressed, and such person's response to the act is one of a person of average sensibilities considering the age of such person."[117]

This statute is a good model for legislating against abusive online conduct. It covers multiple communications media, including the Internet. It also focuses on the victim's state of mind. While several of the sub-sections require the victim to actually be the recipient of the harasser's communications,[118] the final sub-section does not require a communication directed to the victim.[119] Thus, it could cover a situation where the harasser poses as the victim online and incites third parties to harass the victim. That sub-section also includes a reasonableness requirement with respect to the victim's response. For liability to attach, the victim's response should be appropriate to a person of "average sensibilities considering the age" of the victim.

One problematic aspect of the statute is that it is not limited to situations in which the harasser engages in a repetitive pattern of abusive conduct towards the victim. Thus, it might catch a one-time situation where a perpetrator acts out of character in the heat of the moment.[120] This may be a factor that courts should consider in applying the statute, even though the express words of the statute do not require the courts to identify a pattern of abusive conduct. Additionally, there is no express "legitimate expression" defense. Courts applying the statute may thus need to consider, in any given case, whether the defendant's speech should be protected on constitutional grounds.

4. Drafting Effective Criminal Legislation

Criminal laws focused on online abuses need to deal with a number of issues that many state and federal laws are currently lacking. The laws need to remove requirements of proximity to the victim, and requirements of a credible threat of physical harm in order to be effective in cyberspace.[121] Legislators may want to retain some laws with a credible

---

[117] Missouri Ann. Stat. § 565.090(1) R.S. Mo. (2009).

[118] *id*, § 565.090(1)(3) & (4).

[119] *id*., § 565.090(1)(6).

[120] SUTTON, *supra* note 114, at 11.

[121] Schwartz, *supra* note 19, at 429 ("none of the crimes should require an element of proximity to the victim, nor should they include an 'overt' or 'credible' threat requirement"); Goodno, *supra* note 39, at 136 ("In cyberstalking cases, a statute with a credible threat requirement does not protect against electronic communications (such as

threat requirement because such laws may be less open to First Amendment challenge than laws of more general application. However, where legislators have focused on credible threat provisions, resulting laws will have to be supplemented with other regulatory approaches that remedy situations where there is no direct and immediate threat to a victim.[122]

Cyber-abuse laws might also usefully include a requirement of repetitive conduct to avoid catching situations where a person feeling unconstrained by the online medium acts in a one-time capacity without any ongoing intent to threaten or harass another.[123] Of course, some of these one-time communications can lead to permanent and lasting damage because of the global and permanent nature of online information disclosures.[124] Legislators will need to strike a careful balance to ensure that trivial comments are not sanctioned while more damaging one-time activities can be appropriately deterred.

There may be a number of ways to achieve this balance. For instance, judges could be asked to focus on the substance of the online communication in terms of whether the statements made by the perpetrator are likely to cause minor annoyance or major harm to the victim. A comment that someone is "not a nice person" is less egregious than a comment that someone is a "slut" or that she "wants to be raped". Legislation could be drafted to give judges discretion to punish one-time

---

thousands of e-mail [sic] messages) that are harassing, but do not include an actual threat."); 138 ("A second problem with a credible threat requirement in cyberstalking cases is an issue of receipt. A 'threat' suggests a communication directly from the stalker to the victim. But a cyberstalker can easily post terrifying messages without ever being in direct contact with the victim or without the victim ever personally receiving the message…. A third problem that the credible threat requirement creates in cyberstalking case is that it requires the victim to prove that the cyberstalker had the 'apparent ability' to carry out whatever he threatens. What if the cyberstalker sends a threatening e-mail [sic] to the vicim from across the country? It would seem that the victim might then have the burden to prove that the cyberstalker had the financial ability to buy a plane ticket to travel across the country to carry-out [sic] that threat. Such a requirement is onerous and unnecessary, particularly since the victim may not even know the true identity or location of the cyberstalker.").

[122] See discussion in Part III, *infra*.

[123] Schwartz, *supra* note 19, at 430 ("the applicable actus reus [for cyber-victimization crimes] should include a requirement of repetitive conduct. It is important that repetition be incorporated for all of the crimes because 'punishing merely one instance of harassing conduct may unjustly penalize one who acts once out of anger, verses one who engages in a series of terrifying acts".); SUTTON, *supra* note 114, at 11.

[124] Citron, *Mainstreaming Privacy Torts*, *supra* note 7, at [9] (describing permanence of information posted online); Lipton, *We, the Paparazzi*, *supra* note 4, at 977 (describing use of Internet archives to maintain permanent records of information posted online)

offenders in cases where their online communications are particularly egregious. Another approach would be for legislation to require that the proscribed conduct should *generally* be of a repetitive nature, while not expressly preventing a judge from sanctioning stand-alone communications in appropriate cases.

Legislation aimed at online abuses should also maintain the *mens rea* requirements that currently exist in state legislation. For example, the Nebraska statute described in Part II.A.2 requires willful conduct on the part of the perpetrator.[125] This may go some way towards mitigating any perceived harshness inherent in allowing judges to sanction one-time abuses. Judges might utilize the *mens rea* requirement to distinguish activities that rise to the level of criminal conduct from those resulting from a brief burst of anger.

Effective legislation should not require a communication to be sent directly to the victim.[126] Web technologies including blogs, online social networks, wikis, and other online discussion forums are extremely popular. However, they generally do not involve communications sent directly to another. Rather, communications are posted for the whole world to see, or, in a closed network, for a particular community to see, such as a community of "Facebook friends".[127] Communications sent directly to another might merit special attention, particularly if they involve direct and credible threats of harm. However, direct threats are not the sum total of today's damaging online conduct.

Any attempt to legislate against online abuses must be sensitive to First Amendment concerns. Legislation aimed at prohibiting immediate and credible threats is less likely to be unconstitutional than legislation of broader application. In the cases of broader legislation, the First Amendment might be accommodated by ensuring that the legislation specifies that the speech in question is not constitutionally protected.[128]

---

[125] Neb. Rev. Stat. § 28-311.03 (2010) (" Any person who willfully harasses another person or a family or household member of such person with the intent to injure, terrify, threaten, or intimidate commits the offense of stalking.")

[126] Goodno, *supra* note 39, at 146 (noting problems with current anti-cyberstalking statutes in Louisiana and North Carolina in that those statutes require harassing communications be sent 'to another').

[127] Lipton, *We, the Paparazzi*, *supra* note 4, at 939 (describing the concept of Facebook "friends").

[128] Schwartz, *supra* note 19, at 431-432; see Fla. Stat. § 784.048(1)(b) (2009) ("'Course of conduct' means a pattern of conduct composed of a series of acts over a period of time, however short, evidencing a continuity of purpose. Constitutionally

While it may be difficult to perfectly accommodate the First Amendment, free speech concerns should not be used as an argument against protecting victims. In the physical world, statutes have successfully criminalized offline analogs to many of today's online wrongs.[129] There is no reason why judges cannot continue to draw lines between protected and prohibited speech in the online context.

Another factor that might usefully be incorporated into future legislation would be the concept of a reasonable person standard relating to the victim's state of mind.[130] If criminal liability only arises when a victim *reasonably* fears for his or her safety, this may protect expression that could not reasonably be regarded as creating fear or emotional distress in the victim's mind. Thus, unpleasant but predominantly harmless online gossip would be protected, but speech that involves, say, egregious damage to a victim's reputation would be sanctioned. The Missouri anti-harassment legislation passed in the wake of the Megan Meier incident is a good example of the incorporation of a concept of the victim's reasonable response to the perpetrator's actions.[131] While reasonable person standards can be difficult to apply in practice, they do give the courts some flexibility in deciding which conduct to sanction and which conduct should be excused.

B. Tort Law

1. Online Abuses: Common Challenges for Tort Law

Cyberspace interactions pose challenges for tort law, including defamation,[132] privacy torts,[133] and intentional infliction of emotional

---

protected activity is not included within the meaning of 'course of conduct.' Such constitutionally protected activity includes picketing or other organized protests."); Fla. Stat. § 748.048(1)(d) (2009) ("'Cyberstalk' means to engage in a course of conduct to communicate, or to cause to be communicated, words, images, or language by or through the use of electronic mail or electronic communication, directed at a specific person, causing substantial emotional distress to that person and serving no legitimate purpose.")

[129] See, for example, statutes discussed in Part II.A.2, *supra*.

[130] Goodno, *supra* note 39, at 139-140 ("Those stalking statutes that have a reasonable person standard provide the most successful way to prosecute cyberstalking …. The reasonable person standard does not require that the cyberstalker send an explicit threat to the victim, nor does it require that the victim prove the cyberstalker had the ability to carry it out. Instead, the standard focuses on the victim and whether it is reasonable for her to fear for her safety because of the cyberstalker's conduct.")

[131] Missouri Ann. Stat. § 565.090(1) R.S. Mo. (2009); see discussion in Part II.A.3, *supra*.

[132] Citron, *Cyber Civil Rights, supra* note 5, at 87 ("Targeted individuals [of online

distress.[134] The common challenges to all of these torts include the ease with which a perpetrator can hide his identity by utilizing a pseudonym and anonymizing technologies, making it difficult to locate and identify him.[135] While it is possible to unmask anonymous actors online,[136] often much damage has been done by the time the actor is identified.[137] Unmasking a perpetrator of an online abuse may require a court order. This can be expensive and time consuming, outside the budget of many victims of cyber-abuses.[138]

Another practical problem raised by anonymous and pseudonymous online communications is the fact that some plaintiffs may use tort law to unmask the author of defamatory comments not with a view to proceeding

---

abuses] could … pursue general tort claims, such as defamation. False statements and distorted pictures that disgrace plaintiffs or injure their careers constitute defamation per se, for which special damages need not be proven."); Lyrissa Lidsky, *Silencing Jon Doe: Defamation and Discourse in Cyberspace*, 49 DUKE L J 855 (2000) (expressing concerns that defamation suits will be the obvious actions to combat online abuses and will potentially stifle online discourse); Kara Carnley-Murrhee, *Sticks & Stones: When Online Anonymous Speech Turns Ugly*, UF LAW, 21, 22 (Winter 2010) (citing Lyrissa Lidsky describing the ease of bringing defamation actions for objectionable speech online) [hereinafter, *Sticks and Stones*]

[133] Carnley-Murrhee, *Hot Air, supra* note 7, at 19 (citing Scott Bauries noting that tort actions for invasion of privacy might be a useful approach to cyberbullying)

[134] Citron, *Cyber Civil Rights, supra* note 5, at 87-88 ("Many victims [of online abuses] may have actions for intentional infliction of emotional distress. That tort responds to 'extreme and outrageous conduct' by a defendant who intended to cause, or recklessly caused, the plaintiff's severe emotional distress …. Various types of online harassment have supported emotional distress claims, including threats of violence, the publication of a victim's sensitive information, and disparaging racial remarks."); Lyrissa Lidsky, Comments on Blog Posting: *New Cyberbullying Case: D.C. v R.R.*, March 19, 2010, available at http://prawfsblawg.blogs.com/prawfsblawg/2010/03/new-cyberbullying-case-dc-v-rr.html#comments, last viewed on March 22, 2010 (noting that intentional infliction of emotional distress is relevant to new cyberbullying case).

[135] For example, the TOR anonymizing software: See http://www.torproject.org/overview.html.en#thesolution, last viewed on April 14, 2010 ("Individuals use Tor to keep websites from tracking them …"); see also FERTIK and THOMPSON, *supra* note 1, at 71 (discussion of anonymizing technologies, including TOR).

[136] Some examples of "unmasking" litigation: *Columbia Ins Co v SeesCandy.Com*, 185 F.R.D. 573 (N.D. Cal. 1999) (attempt to identify anonymous domain name cybersquatter); *In re Subpoena Duces Tecum to America Online*, 52 Va. Cir. 26 (2000) (attempt to unmask anonymous online defendants); *In re Verizon Internet Services*, 257 F. Supp 2d 244 (D.D.C. 2003) (attempt to unmask anonymous online copyright infringers under subpoena provisions in 17 U.S.C. § 512).

[137] For example, in the Megan Meier case, the victim had already committed suicide by the time Lori Drew's actions were investigated: See discussion in Part II.A.3, *supra*.

[138] Lidsky, *John Doe*, *supra* note 8, at 1387 (noting that many victims of online defamation, for example, lack the resources to bring suit).

with the litigation, but rather with the intention of taking matters into their own hands. Thus, instead of the judicial system working to compensate the victim for the harm she suffered, it creates a platform for her to engage in a campaign of vigilante justice against the defendant. Even in situations where the victim herself does not intend to use the defendant's identity to retaliate, the unmasking could lead to others engaging in online attacks against the defendant.

Basically, any legal action used to identify anonymous speakers runs the practical risk of creating a backlash against the speaker, regardless of whether the speaker might have a valid defense to a tort action. Whether or not the action goes forward, both the plaintiff and the defendant face a potential barrage of new online attacks as a result of the public nature of the lawsuit.[139] Many of the extra-legal approaches to protecting online reputations discussed in Part III do not involve publicity of the original abusive incident and thus avoid the potential for retaliatory attacks against those involved in the original incident. Any tort-based litigation will also involve time and costs that an individual victim may not be in a position to bear.[140] Along with these burdens, a victim would have to relive the shame and humiliation of the abuse in the public record during the proceedings.[141]

---

[139] Bartow, *supra* note 14, at 386-7 ("The targeted law students [in the *AutoAdmit* case] were apparently initially ridiculed on AutoAdmit by people they knew in real space, as evidenced by personal information that was disclosed, such as the style or color of clothing they wore at a particular location. But once the women were contextually framed as people who deserved to be mocked and punished (mostly because they objected to the ill treatment [by commencing litigation]) online strangers mobbed and besieged them as well."); 399 ("[W]hen women complain about harassment, it often escalates. The AutoAdmit administrators seemed to intentionally create a climate the encouraged angry, widespread flaming of anyone who complained about the way they were treated by posters at the AutoAdmit boards. This intensified the harassment, which in turn led to the filing of the lawsuit. Subsequently, seemingly everywhere in cyberspace that the AutoAdmit lawsuit was discussed where anonymous commenting was allowed, attacks on the two women [who were victims of the online abuse] followed.")

[140] *id*; Citron, *Cyber Civil Rights, supra* note 5, at 90 (noting that many plaintiffs in the cyber-harassment context cannot afford the high costs of litigation); Schwartz, *supra* note 19, at 427 ("Furthermore, even if there is an applicable cause of action, the simple well-known fact that 'civil lawsuits are expensive' will often prevent injured parties from bringing suit based on limited resources. As part of her story about being targeted by an internet stalker, Cynthia Armistead states: 'Legal advisors have since told me that there was more than enough evidence to obtain a civil judgment, but I did not have the resources to pursue a civil case ... when the case was "fresh".' Armistead's perspective, as someone who has directly faced internet abuse, highlights the fact that costs and difficulties of maneuvering and understanding the legal system present hurdles that would impede many victims from pursuing civil redress.")

[141] Lipton, *We, the Paparazzi*, *supra* note 4, at 961 (Noting that plaintiffs are put in the awkward position of having to relive the humiliation and embarrassment of the images

While attempting to punish the wrongdoer, the victim would effectively be drawing more attention to the harmful conduct.

Victims of online abuses also face jurisdictional hurdles. Even in cases where the victim knows, or is able to ascertain, the identity of the perpetrator, that party may be in another jurisdiction. Courts in the victim's place of residence may not be able to assert jurisdiction over out-of-state defendants. The costs to the victim of establishing jurisdiction over the defendant, often coupled with the costs of identifying the defendant in the first place,[142] may be prohibitive. Even in cases where the victim is able to identify and assert jurisdiction over an out-of-state defendant, the enforcement of an award for damages or an injunction may be another matter. In many cases it will be impossible or impracticable to enforce a judgment against a remote or impecunious defendant.

Another general limitation of tort law is the difficulty associated with attaching liability to parties who provide forums for posting damaging content. These parties are generally immune from liability for the speech of others under § 230 of the Communications Decency Act (CDA).[143] Section 230 immunizes providers and users of "interactive computer services" from liability for information "provided by another information content provider".[144] In other words, where an entity has provided a forum for online speech, that entity shall not be held liable for tortious speech of others who may use the forum for harmful purposes.[145]

Section 230 presents challenges for victims of online abuse both because it immunizes the most obvious party against whom an injunction could be enforced and because it has been very broadly interpreted by the

---

as they are entered into the public record as part of the court proceedings.); Lidsky, *supra* note 8, at 1390 ("suing often brings more attention to libelous statements").

[142] Lidsky, *John Doe*, *supra* note 8, at 1385 (noting uncertain state of law applying to the unmasking of anonymous defendants, which would also add to the costs of unmasking defendants in interstate cases).

[143] 47 U.S.C. § 230(c)(1) (2000) ("No provider or user of an interactive computer service shall be treated s the publisher or speaker of any information provided by another information content provider.")

[144] *id*.

[145] Citron, *Mainstreaming Privacy Torts*, *supra* note 7, at [39] ("Website operators will enjoy immunity from tort liability under section 230(c)(1) of the Communications Decency Act …. Section 230 generally frees online service providers from liability related to the postings of others."); FERTIK and THOMPSON, *supra* note 1, at 6 ("A legal loophole in the Communications Decency Act makes it impossible to force a website to remove anonymous attacks, no matter how false and damaging they may be.")

courts.[146] Online service providers are the most effective points in the chain of communications for victims to pursue. They provide the gateways for online discourse. Victims of online abuses can easily identify them. They generally have the financial resources to compensate victims by way of damages and, more importantly, they usually have the technical capacity to remove abusive postings and block abusive posters.

However, under § 230, courts have immunized online service providers from defamation and associated liability for extremely egregious conduct, including comments posted by those with whom the ISP may have a close contractual relationship.[147] Further, the near-absolute immunity[148] of online service providers under § 230 has had the practical effect of preventing courts from engaging in meaningful discussions of the standard of care that might be expected of these service providers absent the statutory immunity.[149] While § 230 immunizes intermediaries and disincentivizes them from monitoring online postings, a victim may effectively have no legal remedy at all in cases where an anonymous poster cannot be found. There will be no action available against the intermediary and no way of bringing an action against the original poster of the abusive content.[150]

2. Defamation

---

[146] *Zeran v America Online*, 129 F. 3d 327 (4th Cir 1997) (immunizing Internet service provider from false and defamatory comments posted by others even in circumstances where it had knowledge of the postings and had not acted swiftly to remove them, because of a broad application of § 230 of the Communications Decency Act); *Blumenthal v Drudge*, 992 F. Supp 44 (D.D.C. 1998) (holding that America Online was not liable for comments posted by a commentator it had contracted with to make sensationalist comments on its services because of the application of § 230 of the Communications Decency Act).

[147] *Blumenthal v Drudge*, *supra* note 132.

[148] Internet service provider has not been absolute as a result of the application of § 230 of the Communications Decency Act. In *Fair Housing Council of San Fernando Valley v Roommates.com*, 521 F. 3d 1157 (9th Cir, 2008), an online service provider was held liable for information that it had created in part. See also Citron, *Mainstreaming Privacy Torts*, *supra* note 7, at [39] ("Section 230 generally frees online service providers from liability related to the postings of others. This safe harbor is inapplicable, however, if the website operator helps create the content enabling the criminal activity. The anti-abortion group running the *Nuremberg Files* site exemplifies a party with no immunity under section 230.")

[149] Citron, *Cyber Civil Rights, supra* note 5, at 116-117 ("[The] efforts to read a sweeping immunity into § 230 despite its language and purpose have prevented the courts from exploring what standard of care ought to apply to ISPs and website operators.")

[150] FERTIK and THOMPSON, *supra* note 1, at 65 ("[W]hen the original author cannot be found, the website's refusal to act leaves the victim without any remedy: the false content stays online, forever staining the victim's reputation.")

Defamation law only protects victims against false statements that may harm their reputations.[151] Many online statements are true, even if unpleasant or embarrassing. Many are also statements of opinion which are not typically actionable.[152] Even where the comments are true, the victim in bringing an action puts the defendant to proof on the public record of the truth of the comments. In many cases this could be very awkward for the plaintiff. For example, a defendant may be required to prove that a plaintiff is, in fact, a "slut". Even bringing evidence of more innocuous things, like proof that the plaintiff was overweight, could be highly embarrassing to the plaintiff.

Despite these practical limitations, defamation law – like all laws impacting social conduct - serves an important expressive function that helps to guide conduct between individuals online.[153] Thus, even the possibility of a small volume of online defamation actions may serve a larger regulatory purpose in terms of expressing social values more broadly. If we remain aware of the limitations of defamation as an enforcement mechanism, we might nevertheless accept its important expressive functions.

---

[151] Restatement (Second) of Torts, § 558(a) (requiring a "false and defamatory statement" as an element of a defamation action); § 559 ("A communication is defamatory if it tends so to harm the reputation of another as to lower him in the estimation of the community or to deter third persons from associating or dealing with him.").

[152] *id*., at § 566 ("A defamatory communication may consist of a statement in the form of an opinion, but a statement of this nature is actionable only if it implies the allegation of undisclosed defamatory facts as the basis for the opinion.");Lidsky, *John Doe*, *supra* note 8, at 1382 ("A statement can only be defamatory if it asserts or implies objective *facts* about the plaintiff; otherwise, it will be deemed constitutionally protected opinion.")

[153] Lidsky, *John Doe, supra* note 8, at 1390 (noting that a defamation action can serve the function of creating a fear of being unmasked in other potential defendants, and thus can impact online behaviors with respect to parties outside the litigation process); NEIL NETANEL, COPYRIGHT'S PARADOX, 104-105 (2008) ("[L]aw often serves an expressive or symbolic function above and beyond regulating or providing incentives for conduct. Antidiscrimination law, for example, may have symbolic importance beyond whatever discriminatory conduct it actually proscribes. In enacting and applying such law, Congress and the courts effectively express our society's official condemnation of discrimination based on race and various other classifications. Similarly, the law might forbid certain market transactions, such as selling body parts or children for adoption, not merely to avoid harmful consequences that might ensue but to make a statement about human dignity. Laws that protect endangered species, forbid hate speech, and require recycling also have important symbolic dimensions over and above their regulation of conduct per se. Such laws give vent to and help crystallize collective understandings and norms. In turn, by giving legal imprimatur to certain values, they shape future perceptions and choices.")

3. Privacy Torts

The American privacy torts were developed at a time well before the age of electronic communications technologies.[154] The laws are focused largely on reasonable expectations of privacy drawn from paradigms involving physical space.[155] One may have a reasonable expectation of privacy behind a locked door but may not have such an expectation in a public street. In the electronic sphere, these expectations break down. Is a Facebook page more like a public forum or a private space? While a Facebook user may exert some control over who accesses her profile, surely more people will access that profile than her private house. An individual Facebook user may not know her Facebook "friends" as well as she knows people she invites into her own home. It is not clear how much privacy she actually expects from her online relationships.

Although different states vary on privacy protections, most maintain some variations on the four privacy torts identified by Dean Prosser in 1960.[156] These torts are: (a) intrusion into seclusion;[157] (b) public disclosure of private facts;[158] (c) false light publicity;[159] and, (d) commercial misappropriation of name or likeness.[160] None of these torts is an obvious

---

[154] Citron, *Mainstreaming Privacy Torts*, *supra* note 7, at [3] ("Privacy tort law is a product of prior centuries' hazards. In the late nineteenth century, snap cameras and recording devices provided a cheap way to capture others' private moments without detection. The penny press profited from the publication of revealing photographs and gossip about people's personal lives.")

[155] Patricia Sánchez Abril, *Recasting Privacy Torts in a Spaceless World*, 21 HARVARD JOURNAL OF LAW AND TECHNOLOGY 1, 2 (2007) ("[P]rivacy is usually a function of the physical space in which the purportedly private activity occurred."); 3 ("Traditionally, privacy has been inextricably linked to physical space.")

[156] Dean Prosser, *Privacy*, 48 CAL L REV 383 (1960).

[157] 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.")

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

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

[160] *id*., § 652C ("One who appropriates to his own use or benefit the name or likeness

match for the kinds of conduct examined in this article.

Unpleasant comments about another, whether directed to that other, or directed to a general audience, will generally not be an intrusion into another's seclusion. The intrusion tort is based on notions of intrusion into a person's private physical space, rather than intrusions into a person's mental state.[161] The intrusion tort would generally cover cases where someone has entered another's private domain without invitation. It would be difficult to apply the concept to unpleasant comments made in online forums.[162]

While some commentators have argued that it would not be much of a stretch for courts to extend the tort to conduct like hacking people's password protected email accounts,[163] there is as yet no judicial authority on point.[164] Another potential limitation of the intrusion tort, even if it were extended to online conduct, is that it would likely only apply to intrusions into the plaintiff's own private online spaces, such as the plaintiff's email account or Facebook page. It would be difficult to argue that the plaintiff could make out an intrusion claim where the defendant had simply published unpleasant information about her online without specifically impacting on any area of the plaintiff's own "online space".

The public disclosure of private facts tort is also problematic. This tort deals with the publication of private and non-newsworthy information disclosure of which would be "highly offensive to a reasonable person".[165] This tort may apply to some online abuses, but it is not clear where the line would be drawn in terms of identifying sufficiently offensive information. Courts have generally set the bar relatively high and have imposed a

---

of another is subject to liability to the other for invasion of his privacy.")

[161] Citron, *Mainstreaming Privacy Torts*, *supra* note 7, at [25] ("Plaintiffs cannot bring intrusion into seclusion claims because online postings do not involve invasions of a place that the plaintiff understands as private.")

[162] *id*.

[163] Citron, *Cyber Civil Rights, supra* note 5, at 88 ("Online mobs could face intrusion claims for hacking into password protected e-mail accounts containing private correspondence and conducting denial-of-service attacks to shut down personal blogs and websites.")

[164] In fact, Professor Citron cites a case of an intrusion claim involving a creditor making intrusive phone calls as an example of the extension of the tort away from activities by the defendant that involve the defendant's physical presence in the plaintiff's personal space: Citron, *Cyber Civil Rights*, *supra* note 5, at 88, n. 4 (citing *Donnel v Lara*, 703 S.W. 2d 257, 260 (Tex. Ct. App. 1985)).

[165] Citron, *Cyber Civil Rights, supra* note 5, at 87.

significant burden on plaintiffs to prove offense.[166] While some online communications may meet this test, others will not. For example, photographs of an individual in a sexually explicit and compromising situation may be highly offensive, while comments that a person is fat or slutty, or simply the posting of generally unflattering photographs with unpleasant commentary may not be sufficiently offensive.

False light publicity is also problematic online.[167] It might be regarded as the little brother of defamation law in the sense that it proscribes publication of information that is not, strictly speaking, false, but that may present an individual in a false light. Litigants will be forced to argue on the public record about the truth or falsity of unpleasant comments and the extent to which recipients of the information formed a false impression of the plaintiff. As with the public disclosure tort, the false light publicity tort – when coupled with the other disadvantages of litigation – is only a limited answer to online abuse.

It is unlikely that the misappropriation tort would apply to much online harassment because this tort requires the defendant to have made an unauthorized commercial profit from the plaintiff's name or likeness.[168] Most online abuse is non-commercial. It is possible that a plaintiff might bring an appropriation action against that the operator of a web service that made money from encouraging personally hostile discourse. For example, a service like AutoAdmit or Juicy Campus[169] – if it adopted a commercial model based on advertising or membership fees and then facilitated abusive online discussions - might be said to be making a commercial profit from another's name or likeness. However, a court may require that the defendant itself be the person who appropriated the plaintiff's name or likeness. Where the defendant has rather provided a forum for others to

---

[166] Lipton, *We, the Paparazzi*, *supra* note 4, at 932 ("The [public disclosure] tort also generally requires that the private facts in question must have been shameful by an objective standard which is often difficult to prove."); Jonathan B Mintz, *The Remains of Privacy's Disclosure Tort: An Exploration of the Private Domain*, 55 MARYLAND LAW REVIEW 425, 439 (1996) ("Whether a fact is private by nature - that is, whether a reasonable person would feel seriously aggrieved by its disclosure - is the subject of some disagreement.")

[167] Citron, *Mainstreaming Privacy Torts*, *supra* note 7, at [25] ("False light claims require proof of plaintiff's placement in a false light. They do not apply when … leaked information causes mischief because it is true.")

[168] 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.")

[169] Cohen-Almagor, *supra* note 3, at 11-14 (discussing moral responsibility of services like Juicy Campus for harmful postings by their members).

appropriate names and likenesses for abusive discourse and has profited from providing that forum, a court may hold that the elements of the tort are not satisfied.[170] In any event, § 230 of the CDA would immunize most providers of these forums from any such liability.

4. Intentional Infliction of Emotional Distress

The intentional infliction of emotional distress tort may be more promising than the other torts. This tort requires a finding of extreme or outrageous conduct on the part of the defendant that caused, or was intended to cause, severe emotional distress.[171] Some courts have been willing to find for plaintiffs where a defendant exploits a power disparity between the parties or otherwise takes advantage of a vulnerable plaintiff.[172] It may be easier to convince a court of such a power disparity or vulnerability in online abuse cases than to focus on the content of the communication, which is generally necessary in defamation and some of the privacy torts.[173]

While it is difficult to determine by contemporary social standards what might satisfy the extreme or outrageous conduct limb of the tort, many cases of cyberbullying and cyber harassment will have powerful emotional effects on their victims. For example, a recent situation involving the "Casual Encounters" board on Craigslist resulted in a teenager being inundated with pornographic messages and confronted by men at her place of work as a result of an online posting that she had rape fantasies and enjoyed pornography.[174] Even though the perpetrator's conduct involved merely posting a message on Craigslist, his action – coupled with the substance of the message and the harmful results – may amount to extreme or outrageous conduct. Although the intentional infliction of emotional distress action may theoretically be a promising avenue for individuals harmed by cyber abuses, this tort still suffers from the same practical limitations as the other torts in terms of time, cost, jurisdictional challenges,

---

[170] But see Citron, *Mainstreaming Privacy Torts*, *supra* note 7, at [35-43] (suggesting the development of an action for tortuous enablement of criminal or tortuous conduct by website operators).

[171] Citron, *Cyber Civil Rights*, *supra* note 5, at 87-8; Restatement (Second) of Torts § 46(1)(1965).

[172] Citron, *Cyber Civil Rights, supra* note 5, at 88 ("Courts are more willing to consider conduct 'outrageous' if the defendant exploited an existing power disparity between the parties or knowingly took advantage of a vulnerable plaintiff").

[173] For example, defamation actions and false light publicity claims focus, at least in part, on the *content* of the communications made by the defendant about the plaintiff.

[174] Citron, *Mainstreaming Privacy Torts*, *supra* note 7, at [15].

and potential increased public humiliation for either or both parties.

C. Civil Rights Law

Professor Citron has recently suggested that a civil rights agenda might be developed to combat certain cyber abuses.[175] Civil rights laws include doctrines against race discrimination that might interfere with a victim's ability to make a living and laws that criminalize threats of force designed to intimidate or interfere with a person's employment based on that person's race, religion or national origin.[176] In other words, civil rights law addresses the kinds of conduct typically described as harassment in the sense that victims are targeted because of their membership in a particular protected class.[177] Title VII of the Civil Rights Act of 1964 prohibits gender discrimination as a result of intimidation, threats or coercion aimed at interfering with employment opportunities.[178] While this law focuses on employment opportunities, many online abuses aimed at women and minorities do prevent members of those groups from engaging in employment or "making a living" because many people's businesses are now conducted wholly or partly online.[179]

Civil rights suits entail some advantages including easing the costs of litigation for victims of online harassment,[180] as well as reaching wrongs

---

[175] Citron, *Cyber Civil Rights, supra* note 5, at 89 ("A meaningful response to abusive online mobs would include the enforcement of existing civil rights laws …")

[176] *id*., at 91-92 (citing 42 U.S.C. § 1981 and 18 U.S.C. §245(b)(2)(C) respectively).

[177] See discussion in Part I.A.3, *supra*.

[178] Citron, *Cyber Civil Rights*, *supra* note 5, at 92 ("Gender discrimination that interferes with a person's ability to make a living can be pursued under Title VII of the Civil Rights Act of 1964, which sanctions those who intimidate, threaten, or coerce, or attempt to intimidate, threaten, or coerce someone with the purpose of interfering with employment opportunities due to their gender.")

[179] *id*. ("Destructive online crowds intimidate women and members of racial and religious minorities, preventing them from 'making a living' due to discriminatory animus. Because the Internet fuses our public and private lives and is a workplace for many, online attacks on vulnerable individuals often interfere with their equal right to pursue work. For instance, women who stop blogging in the face of an online mob's attack lose advertising revenue and opportunities for advancement….Online mobs also conduct denial-of-service attacks to shut down blogs that generate income for women and racial minorities. They spread damaging statements to employers and professors for whom victims may work in order to interfere with their employment opportunities."); Madden and Smith, *supra* note 57, at 3 (noting that 12% of employed adults now report that they need to promote themselves online).

[180] Citron, *Cyber Civil Rights*, *supra* note 5, at 92 ("[C]ivil rights laws have attractive remedial features. Because damages may be hard to prove and quantify, and because many plaintiffs cannot afford to litigate based on principle alone, the high cost of litigation often

that would otherwise escape criminal or tort liability.[181] However, while Citron's suggested civil rights agenda is well reasoned it remains untried. Adopting a broader civil rights agenda aimed at online abuses would confront many of the same problems as extending tort and criminal law to cover online abuses. Enforcing authorities, including judges and, in some cases the United States Attorney General,[182] would have to be willing to act against online abusers. These authorities may be reticent to do so absent a clearer mandate. Additionally, civil rights laws, along with tort and criminal law, raise problems of identifying often anonymous defendants.

Civil rights law, if applied online, might help some groups targeted by online abusers, such as women, and racial and religious minorities. However, other sets of common victims, such as children, are unlikely to be covered here unless an individual victim also happens to fall into a statutorily protected class. In other words, civil rights law might provide some protections against cyber-harassment, but not necessarily against cyberbullying. As noted above, cyberbullies generally target individuals for reasons outside membership in a protected class.[183] Bullies may target people who they perceive as a threat, or who they regard as weak – potentially including people who are poor, inarticulate, overweight, or socially inept. None of these traits would fall within the umbrella of civil rights protection.

III. Extra-Legal Approaches to Online Wrongs

A. The Need for a Multi-Modal Approach

Because of the limitations inherent in the legal system, a broader multi-modal regulatory approach is necessary to combat online abuses. The idea of combining regulatory modalities in cyberspace is not new.[184] However,

---

deters the filing of general torts suits. The awards of attorney's fees possible under many civil rights statutes might make some cases affordable to pursue.")

[181] *id*. ("[C]ivil rights suits may reach wrongs that would otherwise escape liability. These include victims' rights to be free from economic intimidation and cyber harassment based on race and gender.")

[182] *id*. (noting that the Attorney General can file civil suits for injunctive relief under Title VII of the Civil Rights Act of 1964).

[183] See discussion in Part I.A.2, *supra*.

[184] Lawrence Lessig, *The Law of the Horse: What Cyberlaw Might Teach*, 113 HARV L REV 501 (1999) (suggesting four regulatory modalities for cyberspace: legal rules, social norms, market forces, and system architecture); Lawrence Lessig, *The Architecture of Privacy*, 1 VANDERBILT J ENT L & PRAC 56, 62-3 (1999) (suggesting the same four norms of regulation for online privacy); Lipton, *We the Paparazzi*, *supra* note 4, at 925 ("This Article argues that legal regulation alone is unlikely to solve society's video privacy

web 2.0 technologies increase the need for a complex interplay of regulatory approaches in order to identify, and facilitate the development of, appropriate online behaviors.[185] Relevant regulatory modalities will likely include social norms,[186] system architecture,[187] market forces,[188] public education,[189] and the use of private institutions.[190]

In global online communities laws must interact with other regulatory modalities to achieve a comprehensive approach to combating abuses. Legislators and judges will learn much from observing the development of market solutions,[191] technological solutions and emerging

---

problems. It advocates a multi-modal approach that combines six regulatory modalities: legal rules, social norms, system architecture, market forces, public education, and private/non-profit institutions.").

[185] See, for example, LAWRENCE LESSIG, CODE VERSION 2.0 (full text available at http://pdf.codev2.cc/Lessig-Codev2.pdf, last viewed on April 20, 2010), at 5 ("Cyberspace demands a new understanding of how regulation works. It compels us to look beyond the traditional lawyer's scope—beyond laws, or even norms. It requires a broader account of 'regulation,' and most importantly, the recognition of a newly salient regulator. That regulator is the obscurity in this book's title—Code.") [hereinafter, CODE].

[186] Katherine Strandburg, *Privacy, Rationality, and Temptation: A Theory of Willpower Norms*, 57 RUTGERS L REV 1235,1238 (2005) ("Social norms are primarily understood as means to coordinate the behavior of individuals in a social group. Thus, norms may help to solve coordination problems – by determining how pedestrians pass one another on the street - and collective action problems – by stigmatizing littering - when individually rational behavior leads to collectively undesirable results."); Jacqueline Lipton, *Copyright's Twilight Zone: Digital Copyright Lessons from the Vampire Blogosphere*, forthcoming MARYLAND LAW REVIEW, 2010 (discussing the development of norms of authorship and fan use of copyright works online); Jacqueline Lipton, *What Blogging Might Teach About Cybernorms*, forthcoming AKRON INTELLECTUAL PROPERTY JOURNAL, 2010 (discussing the development and identification of norms in the blogosphere); Steven Hetcher, *Using Social Norms to Regulate Fan Fiction and Remix Culture*, 157 PENN. L. REV. 1869 (2009) (discussing the role of norms in regulating online fan fiction and remix communities); Mark Schultz, *Fear and Norms and Rock & Roll: What Jambands Can Teach Us About Persuading People to Obey Copyright Law*, 21 BERKELEY TECH L J 651 (2006) (discussing the role of norms in regulating copyrights in certain sectors of the music industry).

[187] LESSIG, CODE, *supra* note 185, at 5; Joel Reidenberg, *Lex Informatica: The Formulation of Information Policy Rules Through Technology*, 76 TEXAS L REV 553 (1998) (describing how digital technology can be utilized as a form of regulatory mechanism for online conduct).

[188] Ann Carlson, *Recycling Norms*, 89 CALIF L REV 1231, 1253 (2001) ("Markets constrain behavior through price. If the price of gasoline rises dramatically, people will drive less.")

[189] Lipton, *We, the Paparazzi*, *supra* note 4, at Part IV.E.

[190] *id*., at Part IV.F.

[191] For example, reputationdefender.com, last viewed on May 20, 2010; youdiligence.com, last viewed on May 20, 2010; udiligence.com, last viewed on May 20, 2010 (examples of private online reputation management services).

social norms[192] that impact online behavior. Participants in online communities will also learn something from a legislature's willingness to legislate to proscribe certain conduct. Public education, both through news stories and other means – such as publicly or privately funded education initiatives – are also an important part of the framework. Appropriately tailored educational initiatives will assist in the development of online norms.

This Part examines several extra-legal regulatory approaches that could impact ways in which people interact online. It focuses on regulatory modalities that can empower victims to control their own reputations online. It also suggests ways in which public and private funding might be usefully funneled into educational initiatives to assist individuals in preventing online harms, abuse reporting hotlines, and programs that facilitate relevant industry self-regulation. One advantage of focusing on extra-legal initiatives is that their development is less likely to be hindered by concerns about the First Amendment than legal developments. This is because private actors such as reputation management services and private education providers are not generally subject to First Amendment guarantees.[193]

B. Empowering Victims to Combat Online Abuses

1. Reputation Management Techniques

"Your online reputation is your reputation. Period." [194]

A key to protecting individuals from online abuses is to empower those individuals to protect themselves without needing to resort to the legal system. There are a variety of ways in which individuals can guard their own reputations online. Some methods involve learning to control information that an individual releases about herself on the Internet – such as personal anecdotes and photographs. Educating individuals about the risks of disclosing private information online is an important aspect of protecting online reputation. For example, individuals can be encouraged

---

[192] See, for example, ownwhatyouthink.com, last viewed on May 20, 2010 (campaign to promote more accountable and responsible online discourse).

[193] Constitution of the United States, Amendment I ("Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble, and to petition the government for a redress of grievances.")

[194] FERTIK and THOMPSON, *supra* note 1, at 16.

to use maximum privacy protections on services like Facebook[195] and to ensure that they have sufficient security measures installed on their personal computers to prevent others from accessing their personal information. Individuals can also be trained to build positive online content about themselves as a form of online insurance to prevent negative content from making it into the first page of search results about them.

Better educating people about the risks inherent in releasing their personal information online is unquestionably important. However, bigger problems occur when the individual's friends or acquaintances disseminate the harmful information. While a potential victim may secure her own computer and may be careful about what she discloses about herself online, she has very little control over what others disclose about her. She also has very little control over attacks directed specifically to her.

Individuals now have to be vigilant not only about what they disclose about themselves online, but also in monitoring what others may be disclosing about them.[196] Individuals may also need to be aware of currently available ways to combat damaging content about them. This may involve learning how to conduct a personal reputation audit[197] and asking providers of online forums to monitor, police, and remove damaging content.[198] It may also involve knowing how to use other online tools, such as astroturfing and search engine optimization to repair damage.[199]

Astroturfing involves seeding the Internet with positive or neutral content generated by the individual herself in an attempt to drown out the abusive content.[200] Search engine optimization techniques involve the

---

[195] In fact, Facebook has recently simplified its privacy settings to better enable its users to make use of its privacy-protecting technologies: Mark Zuckerberg, *Making Control Simple*, THE FACEBOOK BLOG, May 26, 2010 (available at http://blog.facebook.com/blog.php?post=391922327130, last viewed on June 7, 2010).

[196] Robert McGarvey, *Is Bad Taste the New Taste? Social Media is Changing Our Sense of What's Acceptable – and What's Not*, THINK 25, 26-27 (Spring/Summer, 2010) (describing situation where an Ohio executive found out that an old friend had posted online a photo of him in a drunken stupor from his youth, and the steps he attempted to take to have the photo de-tagged from social networking websites); Madden and Smith, *supra* note 57, at 2-3 (noting that individuals are indeed becoming more vigilant over time about self-monitoring and observation of information available about others online).

[197] FERTIK and THOMPSON, *supra* note 1, at Chapter 10.

[198] Bartow, *supra* note 14, at 415 (noting that some people who run online forums do a lot of policing on their own initiative).

[199] *id*., at 426-7.

[200] *id*. (describing the use of astroturfing by reputation management services such as ReputationDefender). The term "astroturfing" has arguably begun to take on negative

manipulation of search engine results so that positive or neutral information is prioritized in searches above harmful information.[201] Many of these tools are currently utilized by private online reputation management services, but there is no reason individuals cannot not learn how to use them without needing to pay the fees charged by the private services.[202] Some literature is now available to assist individuals to learn strategies that commercial reputation management services have typically utilized.[203]

Another mechanism for protecting some aspects of an individual's online reputation is available under the notice-and-takedown provisions of the Digital Millennium Copyright Act (DMCA).[204] These provisions allow a copyright holder to send a notice to a website operator requesting removal of material that infringes a copyright. If the operator complies with the notice, it can avoid copyright infringement liability.[205] The effectiveness of this technique in the hands of a private individual will depend on the extent to which the individual actually holds copyright in damaging text and images about her. In many cases, such materials will have been generated by third parties.[206] Thus, the victim will not have a copyright claim that could support the use of the DMCA.[207]

The ability of an individual to make use of any of the techniques described here will depend on her awareness of the techniques. One of the problems for victims of online abuses has been lack of awareness of how to protect one's own reputation online, outside of resorting to the law or

---

connotations in the sense that some people may now associate it with conduct like seeding the Internet with false political information. However, in the absence of a better term, "astroturfing" is utilized in this paper in reference to seeding any type of positive or neutral information about an individual in an attempt to protect her reputation online.

[201] Bartow, *supra* note 14, at 427 (describing use of search engine optimization techniques by private reputation management services).

[202] *id*., at 421 ("It is doubtful that any reputation defense service offers clients anything that they cannot do for themselves if they have a basic understanding of applicable laws, of the way that search engines function, and of the vulnerability of search engines to targeted manipulation.")

[203] For example the founder and general counsel of ReputationDefender have released a book detailing some strategies for individuals to protect their own online reputations: FERTIK and THOMPSON, *supra* note 1.

[204] 17 U.S.C. § 512(c).

[205] 17 U.S.C. § 512(c)(1)(C).

[206] For example, a person who takes an embarrassing photograph of the victim will generally hold copyright in the photograph: DANIEL SOLOVE, THE FUTURE OF REPUTATION: GOSSIP, RUMOR, AND PRIVACY ON THE INTERNET, 184 (2007) ("Copyright in a photo is owned initially by the person who takes the photo, not by the person whose photo is taken.")

[207] *id.*

engaging the services of a private reputation management company. While private reputation management services unquestionably have a useful place in protecting people's online reputations, they are motivated by profits and they can charge high fees[208] for doing a number of things that private individuals could do on their own if they knew how.[209] Cynically, one might also argue that private reputation management services actually benefit from online abuses and it is in their own commercial interests that online abuses continue to some extent.[210]

2. Education

The increased ability of private individuals to utilize effective methods to protect their own reputations online might put more pressure on private reputation management services to develop new products and services, or to price their services more competitively. The question remains how best to empower private individuals to protect their reputations online. Clearly, some level of public education would be useful. Education might be government funded and targeted at schools and other public institutions[211] – like libraries and universities. It may also be that private non-profit organizations, such as the Electronic Frontier Foundation[212] and the Electronic Privacy Information Center,[213] will play an increasingly important role. Education can focus both on empowering victims to protect their reputations against online attacks and on training participants in online communities to behave in a socially acceptable manner more generally.

---

[208] Bartow, *supra* note 14, at 423-426 (describing fees charged by ReputationDefender for its various services).

[209] *id*., at 421 ("It is doubtful that any reputation defense service offers clients anything that they cannot do for themselves if they have a basic understanding of applicable laws, of the way that search engines function, and of the vulnerability of search engines to targeted manipulation."); FERTIK and THOMPSON, *supra* note 1, Chapters 10-13 (describing ways in which private individuals and small businesses can act to protect their own online reputations).

[210] Bartow, *supra* note 14, at 419 ("[T]he greater the quantity of sexual harassment toward affluent victims that appears on the Internet, the wealthier reputation defense services can become."). Of course, one could make similar arguments about the home security system industry. This industry unquestionably profits from home burglaries. However, that is not to say that they condone the conduct of burglars.

[211] While government regulation of speech generally raises First Amendment concerns, the government is generally able to attach speech-restrictive provisions to funding legislation without running afoul of the First Amendment: *United States v American Library Associaton Inc*, 539 U.S. 194 (2003) (upholding legislation that required Internet filtering as a condition of libraries accepting government funding).

[212] See www.eff.org, last viewed on April 20, 2010.

[213] See www.epic.org, last viewed on April 20, 2010.

A number of private organizations already provide information about online harms as well as providing tools for addressing them. Many of these organizations focus on protecting children from online predators and bullies. For example, NetSmartz provides information to parents, guardians, educators, law enforcement authorities and children about staying safe on the Internet.[214] NetSmartz also offers free multimedia safety presentations that can be used in classrooms and other communities. Its website also links to the Internet Crimes Against Children website,[215] a government sponsored educational initiative to protect children online.

Another service aimed at protecting children online is GetNetWise,[216] which provides information, advice and free online tools for keeping children safe online. It contains an inventory of suggested software tools parents might utilize to protect their children as well as critiques of the available software options. It also provides a suggested contract that parents can enter into with their children containing guidelines to help children stay safe in their online interactions.[217]

C. A Critique of Existing Commercial Reputation Management Services

While an increasing number of services provide free information and tools for combating online abuses, some of the most well known services are the for-profit reputation management services like ReputationDefender, Reputation Hawk, and YouDiligence. Private reputation management services raise some practical concerns, despite the useful function they serve. As noted in the previous section, reputation management services offer a variety of options for protecting individual reputations online. They will monitor an individual's online reputation[218] typically for a monthly fee.[219] They then provide monthly reports to a client summarizing information about the client available online.[220]

---

[214] See www.netsmartz.org, last viewed on May 20, 2010.

[215] See www.icactraining.org, last viewed on May 20, 2010.

[216] See http://kids.getnetwise.org, last viewed on May 20, 2010.

[217] See http://kids.getnetwise.org/tools/toolscontracts, last viewed on July 8, 2010.

[218] Focusing on popular services like MySpace and Facebook: See Bartow, *supra* note 14, at 424 ("ReputationDefender claims it will monitor blogs and sites like MySpace, Facebook, Xenga, Bebo, Flickr, LiveJournal, and many others for any material that might be damaging or distressing to a client …")

[219] *id*., at 424 ("The SEARCH part of [ReputationDefender's] service requires payment of a subscription fee, which costs $14.95 per month, with discounts to people who sign up for one or more years at a time."). YouDiligence currently charges between $9.99

If the service detects information that the client objects to, the service will offer to remove the damaging content from the Internet at a charge relating to each piece of information the client wants to destroy.[221] The information does not have to be untrue to be targeted by the service at the client's request.[222] However, many reputation management services now focus on the removal of slanderous or damaging information, and refrain from removing much information that is true or newsworthy.[223] Most reputation management services regard their techniques for sanitizing a person's online reputation as "proprietary"[224] and do not disclose those techniques publicly.[225] However, their methods likely include: (a) using notice and takedown procedures from the DMCA;[226] (b) contacting blogs

---

and $14.99 per month for its monitoring services: see www.youdiligence.com, last viewed on May 20, 2010.

[220] Bartow, *supra* note 14, at 423 (citing ReputationDefender's "SEARCH" process).

[221] *id.,* at 424 ("The DESTROY aspect of the enterprise costs $ 29.95 per piece of unwanted information, with no guarantee of positive or sustainable results.")

[222] *id.* (noting that ReputationDefender does not require information to be inaccurate, harassing or defamatory in order to remove it; and that the service is prepared "to sanitize any inconvenient truths"); at 425 ("ReputationDefender is also willing to mask or bury accounts of mainstream news stories even if they are true.")

[223] ReputationDefender, Frequently Asked Questions, available at http://www.reputationdefender.com/faq/, last viewed on July 8, 2010 ("Our removal ('Destroy') service is designed to help individuals regain control over unintentionally posted or outdated personal information disclosed to the public Internet, and address potentially libelous, slanderous, defamatory or invasive information about them We do not target news/media articles for removal. Nor do we seek to get government records removed from the Internet. We believe that individuals have the right to express ideas freely, and we support the freedom of the press to inquire fully about issues of legitimate public interest. Given that, we reserve the right to refuse any requests that we believe conflict with these fundamental values. But we also believe that it is the right of individuals to know what others are saying about them, and for private individuals to protect themselves from unintentional, inappropriate, or illegal intrusions of their privacy.")

[224] Bartow, *supra* note 14, at 421 (noting ReputationDefender's reference to its techniques as being "proprietary").

[225] *id.,* at 425 ("ReputationDefender refuses to disclose the exact nature of its so-called destruction tools, and presumably its competitors do as well."). More recently, ReputationDefender has disclosed a number of its reputation management techniques: FERTIK and THOMPSON, *supra* note 1.

[226] Bartow, *supra* note 14, at 421 (discussing use of the notice and take-down provisions of copyright law by online reputation management services); see also discussion in Part III.B, *supra*. In an interview with David Thompson, general counsel of ReputationDefender, he stated that ReputationDefender does not actually use the notice and take-down provisions of copyright law in practice (interview with David Thompson at the 3rd Annual Privacy Law Scholars' Conference, George Washington Law School, Washington, D.C., June 3, 2010).

and other web hosts and asking them to remove damaging information;[227] (c) astroturfing the Internet with newly manufactured neutral or positive information about their clients;[228] and, (d) engaging in search engine optimization techniques to ensure that neutral and positive information about their clients is prioritized in search results.[229]

These services provide a number of advantages over legal solutions to online abuses, including the fact that several of them now have many years of experience with reputation management and have established solid working relationships with websites that host harmful communications.[230] The use of private commercial services does not raise the specter of a First Amendment challenge. As noted in Part II, many laws directed at curtailing online speech may raise First Amendment concerns and may be open to constitutional challenge.[231] Reputation management services also avoid many of the practical problems associated with litigation including jurisdictional challenges and difficulties identifying a defendant in the first place. A commercial service does not need to identify or locate a potential defendant in order to engage in astroturfing or search engine optimization. Resort to a reputation management service also avoids drawing public attention to the damaging content.[232] Harmful content can simply be unobtrusively de-prioritized in search engine results.

---

[227] Bartow, *supra* note 14, at 425 ("In addition to utilizing the notice and take-down procedures of copyright law, another of ReputationDefender's vaunted proprietary techniques is apparently to send e-mails to blogs and websites hosting information that its clients want to disappear.")

[228] *id.,* at 426-427 ("[Astroturf] is Internet content that springs from artificial grass roots (hence the name) and is engineered to falsely appear as originating from diverse and geographically distributed, independently acting individuals. Reputation defense services may be seeding the world wide web with astroturfing websites and blogs of their own creations to create a faux chorus of noise that drowns out speakers that their clients wish would 'sod off,' whether for socially good reasons, or for bad.")

[229] *id.,* at 427 ("Another avenue open to reputation defense organizations is Search Engine Optimizing, which has been characterized by at least one legal scholar as fraud. It is an effort to manipulate search engine results for profit."); Lidsky, *John Doe*, *supra* note 8, at 1390 (describing services provided by commercial reputation management companies).

[230] FERTIK and THOMPSON, *supra* note 1, at 206 ("Professionals have built thousands of websites and know exactly how to optimize them to rank the highest in Google and other search engines. They often know the right tone to strike and the right balance of links to create. And professionals often have an arsenal of deals with specialized websites that allow rapid improvement in search results.")

[231] See, for example, Diane Leenheer Zimmerman, *Is There A Right to Have Something to Say? One View of the Public Domain*, 73 FORDHAM L REV 297, 348-9 (2004).

[232] Lidsky, *John Doe*, *supra* note 8, at 1390 ("Hiring a reputation management

However, reliance by individuals on these commercial services has a number of disadvantages, despite the obvious benefits. One of the key disadvantages relates to cost and equity issues. Many of the victims of online harassment and other abuses will not be able to afford the fees charged by these services.[233] While engaging a service to monitor one's reputation on the Internet may be relatively affordable,[234] paying fees to repair one's online reputation may be prohibitive for many. Additionally, while these commercial services are available – at least to some more wealthy people – there may be less pressure on the government to act. If the government thinks the market is handling the problem, government agencies may put less effort into investigating and prosecuting the abuses.[235]

The apparent availability of reputation management services may also negatively impact the level of monitoring undertaken by those who provide online speech forums. These forum providers are generally immunized from tort liability for the speech of others under § 230 of the CDA.[236] This legislation is a powerful disincentive for online service providers to monitor and act against harmful speech. The perceived availability of reputation management services may further disincentivize online forum providers from monitoring their own forums. Service providers might assume that they need not monitor their forums because not only are they generally immune from legal liability for the speech of their contributors, but also if there is a problem, they will receive a notice from a reputation management service. Better yet, the reputation management service may simply take care of the problem through astroturfing or search engine optimization without requiring any action on the part of the online

---

company sometimes provides an attractive alternative to suing for libel because suing often brings more attention to the libelous statements.")

[233] Citron, *Cyber Civil Rights*, *supra* note 5, at 105 ("Few free or inexpensive services are available for defending one's online reputation, and the services of groups like ReputationDefender are expensive and beyond the means of many victims.")

[234] As noted above, the fees for monitoring one's reputation are typically in the ballpark of around $10 to $15 a month: Bartow, *supra* note 14, at 424 (noting that ReputationDefender charges $14.95 per month to monitor a client's online reputation).

[235] *id.,* at 422 ("While it appears that self-help options are available, momentum for official intervention can dissipate. Government actors may decline to assist online harassment victims because the more affluent ones can theoretically purchase assistance from ReputationDefender or similar services. They may not see a need to step in and have the government provide assistance that could readily be purchased, at least by those who can afford it.")

[236] See discussion in Part II.B.1, *supra.*

service provider.[237] Recent statistics suggest that many online service providers will quickly remove harmful information on request.[238] However, it is difficult to gauge how proactive any of these services are in removing damaging information absent a formal request to do so.

Another practical limitation of reputation management services is that the actions they take to protect their clients' reputations may backfire dramatically. Most of them will not offer any guarantees of success[239] or refunds for backlash caused by their activities.[240] For example, ReputationDefender client, Ronnie Segev, suffered a significant backlash as a result of ReputationDefender's efforts to remove embarrassing content about him from a website.[241] After ReputationDefender sent a notice to the website operator requesting removal of the harmful information,[242] a

---

[237] See discussion in Part III.B, *supra*.

[238] Madden and Smith, *supra* note 57, at 4 (noting that a significant majority of people who have sought removal of information about them posted online have been successful).

[239] The disclaimer in YouDiligence's terms of service is a good example of how little these services guarantee in practice. See YouDiligence.com, Terms of Service, January 5, 2010, clause 14, available at www.youdiligence.com/yd/TermsOfUse.htm, last viewed on May 20, 2010 ("You agree that use of the YouDiligence site and the service is entirely at your own risk. The YouDiligence site and the service are provided on an 'as is' or 'as available' basis, without any warranties of any kind. All express and implied warranties, including, without limitation, the warranties of merchantability, fitness for a particular purpose, and non-infringement of proprietary rights are expressly disclaimed to the fullest extent permitted by law. YouDiligence disclaims any warranties for the security, reliability, timeliness, accuracy, and performance of the YouDiligence site and the service. To the fullest extent permissible by law, YouDiligence disclaims any warranties for other services on the YouDiligence site or the sites or service, or accessed through any links on the YouDiligence site. To the fullest extent permitted by law, YouDiligence disclaims any warranties for viruses or other harmful components in connection with the YouDiligence site or the service.")

[240] Bartow, *supra* note 14, at 424 (noting that reputation management services do not give guarantees of positive or sustainable results); Citron, *Cyber Civil Rights*, *supra* note 5, at 105 ("[I]nstead of slowing down an online mob, counter-measures may sustain the life of the attacks. The very purpose of many online attacks is to force victims off the net; the mobs are likely to respond with particular venom against a victim who not only stays online but tries to fight back. A victim may plausibly conclude that more people will see the defamatory or private material if she responds than if she does not.")

[241] *id*., at 425-427 (discussing the Segev incident).

[242] *id.,* at 426 (citing the text of ReputationDefender's message: "We are writing to you today because our client, Ronnie Segev, has told us that he would like the content about him on your website to be removed as it is outdated and disturbing to him. Would you be willing to remove or alter the content? It would mean so much to Mr Segev, and to us. Considerate actions such as these will go a long way to help make the Internet a more civil place.")

blogger from the website wrote a scathing post entitled "Ronnie Segev and ReputationDefender Can Eat a Dick".[243]

Another limitation of private reputation management services is that they cannot do much in the face of personal attacks directed at a victim, rather than posted publicly online. The tools utilized by reputation management services do not specifically address situations where a person is, say, sending harassing and abusive communications directly to a victim. In the Megan Meier scenario, for example, where harmful communications are directly sent to the victim, there is little that a private reputation management service can do. This may be a situation where legal solutions are more appropriate. Victims of such abuses can, in relevant jurisdictions, rely on cyberbullying and cyber harassment laws if police and prosecutors are prepared to act on the complaints.[244]

D. Effective Reputation Management

1. Enhanced Access to Reputation Management Services

Empowering individuals to fight online abuses themselves requires a number of strategies, many of which rely largely on the availability of funding and public education. For example, pro bono legal services could be encouraged to take on more online abuse cases if they could be staffed and funded to do so. There is also no reason why more pro bono reputation management services could not be developed if government or other funding were available.

The development of more pro-bono reputation management services and public education initiatives would be a useful supplement to currently available commercial reputation management services. As noted above, commercial services are expensive and out of the reach of many victims of online abuses.[245] At the same time, some of the tools they utilize are readily available to private individuals who know how to use them.[246] If victims of online abuses had better information about some of these tools, they could more easily protect themselves online without necessarily having to pay for a commercial reputation management service.

---

[243] *id.*

[244] See discussion in Part I.A, *supra*.

[245] Citron, *Cyber Civil Rights*, *supra* note 5, at 105 (noting often prohibitive expense of utilizing these services)

[246] FERTIK and THOMPSON, *supra* note 1, Chapters 10-13 (advising individuals and small businesses on techniques to self-protect online reputations).

If appropriate funding were available, victims might also have the option of using a pro bono reputation management service. Naturally the choice to pay for a commercial service would still be available. If individuals were savvier about protecting their own reputations online and more pro bono options were available, the commercial services may be incentivized to develop even more sophisticated solutions to online abuses. They would after all be competing for increasingly technologically sophisticated clients with more practical options. This could ultimately lead to the development of new innovations for protecting individual reputations.

Access to existing legal remedies for online abuses might also be improved if pro bono legal services were better equipped to take on these cases. Many legal clinics and other pro bono services might not deal with many of these cases because of unfamiliarity with the relevant laws, or assessment of current law as not adequately covering the victims' harms.[247] A reworking of laws, and increased funding and education to those providing pro bono services to victims of online harassment, might usefully redress the balance here.

2. Cyber-Abuse Hotlines

Another extra-legal approach to protecting online reputation is the increased use of Internet hotlines that can be established on a voluntary basis by various online service providers.[248] Users of online services can be empowered to report online abuses by telephone, fax, email, or submission of an online form. Hotlines should ideally be as confidential as possible, and those who claim abuse should be given some information about how complaints will be handled and the circumstances under which complaints may be referred to a public authority.[249] Of course, this assumes the existence of an appropriate authority to deal with relevant complaints.

The British Internet Watch Foundation exemplifies the hotline approach in reporting illegal online conduct involving certain types of Internet content including: (a) sexual images of children; (b) obscene adult content; (c) material inciting racial hatred; and, (d) inappropriate behavior towards a child online.[250] Users can report such content in a variety of

---

247 Discussion with clinical Professor Laura McNally, March 15, 2010.

248 Cohen-Almagor, *supra* note 3, at 29 (critiquing several existing Internet hotlines).

249 *id*.

250 See www.iwf.org.uk/reporting.htm, last viewed on May 19, 2010.

ways including submission of an online form.[251] In the United States, the CyberTipline is another example of a hotline for reporting certain damaging conduct much of which involves children: for example, child prostitution, child molestation, and sex tourism involving children.[252]

Some of the more salient advantages of hotlines in the context of online abuses include the fact that they can open up channels of communication between victims, observers of harmful conduct, and law enforcement authorities.[253] Hotlines also enable ready collection of data about online abuses including data about the nature of prevalent abuses and demographic characteristics of typical abusers and victims.[254] Hotlines can thus enable law enforcement agencies to gain a clearer picture of online abusive conduct and to target enforcement activities appropriately. Reports generated by hotlines, when released to the public, can also serve an important public education function, increasing awareness of damaging online conduct and enabling individuals, pro bono and private services to develop targeted tools to respond to specific abuses.

3. Evolving Online Norms

Social norms interact with other regulatory modalities in cyberspace as in the physical world. Norms both influence and respond to legal and market developments. For example, a law may alter normative behavior by requiring compliance or simply by expressing appropriate behavioral standards.[255] Markets will often respond to online norms: for example, reputation management businesses developed as society became less civil online and a market demand grew for tools to protect individual reputations. The question today is how to develop norms that foster more civil and accountable online communities.

One approach is to develop online forums that promote community standards of responsibility and accountability. For example, to counter the Juicy Campus debacle,[256] a Princeton student created the "ownwhatyouthink.com" website, asking students to pledge not to visit anonymous gossip sites and to be accountable for their own online

---

[251] *id.*

[252] See www.missingkids.com, last viewed on May 19, 2010.

[253] Cohen-Almagor, *supra* note 3, at 32.

[254] *id*.

[255] See *supra* note 153 (on law's expressive functions).

[256] Cohen-Almagor, *supra* note 3, at 13-14 (describing harmful online postings about college students on the juicycampus.com website).

communications.[257] The site sports the banner headline: "Anonymity = Cowardice".[258]

Of course, norms may work in opposing directions and society – or large sectors of society – may simply become desensitized to many online abuses. As one commentator has noted: "Maybe we soon will simply yawn in boredom the next time we see a tweet typed in an inebriated rant, or a Facebook photo of a friend – or perhaps even ourselves – dancing on a table with bloodshot eyes."[259] Even if we become desensitized to these kinds of communications, one would hope that we never become desensitized to dangerous and harmful conduct like cyberbullying and harassment involving threats of physical harm, or online communications that seriously damage an individual's livelihood or reputation.

4. Industry Self-Regulation

Market self-regulation initiatives may also be an important part of the regulatory matrix. Self-regulation may be adopted voluntarily or may be a result of pressure from customers or from governments. In the cyber-abuse context, the relevant industry is difficult to define. Online abuses occur in a variety of online forums including social networking sites, blogs and even online multi-player games. Search engines like Google will be implicated here because they play such a significant role in determining which Internet users see what information. Self-regulation initiatives in at least some industries might serve an important educational and normative function for those involved in online communications more generally.

Facebook's attempts to use members' information for advertising has been one area where user norms and preferences have often conflicted with Facebook's business plans, and Facebook has attempted to respond accordingly.[260] An example of the interplay between government and market regulation in the social networking context is the 2008 Joint Statement on Key Principles of Social Networking Sites Safety adopted between MySpace and the state Attorneys-General.[261] These principles are aimed at protecting children from inappropriate and harmful online conduct.

---

[257] See www.ownwhatyouthink.com, last viewed on May 19, 2010.

[258] *id.*

[259] McGarvey, *supra* note 196, at 29.

[260] Lipton, *supra* note 4, at 973 (describing user backlash against Facebook's Beacon advertising program); Zuckerberg, *supra* note 195 (describing Facebook's new privacy policies and technological defaults).

[261] Full text available at: http://ago.mo.gov/newsreleases/2008/pdf/MySpace-JointStatement0108.pdf, last viewed on May 21, 2010.

They encompass strategies such as developing software tools to protect children from harmful content,[262] designing social networking sites in a way that prevents minors from accessing inappropriate conduct,[263] educating parents and children about online safety issues,[264] and ensuring that social networking sites cooperate with law enforcement agencies in protecting children online.[265]

Another aspect of self-regulation that could be facilitated by cooperation between online user groups or by government regulation is the prospect of labeling, naming and shaming websites that provide a platform for cyber-wrongs. For example, several years ago in the United Kingdom, the culture minister and her shadow minister presented the idea that online service providers might be named and shamed into dealing more proactively with violent and sexually explicit conduct on their sites.[266] This is a difficult result to achieve in practice because it involves cooperation between a central agency and some realistic pressure brought to bear on websites to take action against harmful online conduct. Additionally, because of the global nature of the Internet, definitions of "harmful conduct" may vary from community to community and country to country. Some countries, with stronger free speech protections, may protect speech that others sanction. Of course, certain speech – like realistic threats of harm – should not be protected anywhere. However, beyond that, it is difficult to draw clear lines about what kinds of conduct should lead to naming and shaming.

Some other recent examples of self-regulation involve Google's relatively new Google Search Wiki and Google Profile service.[267] Google's experimental Search Wiki enables Internet users to make comments on search results.[268] Thus, a victim of reputational harm could use the service to contextualize or refute a criticism made about her. However, the Search Wiki comments are not displayed unless an Internet searcher goes out of his

---

[262] *id*, Principle I.
[263] *id*, Principle II.
[264] *id*, Principle III.
[265] *id*, Principle IV.
[266] Patrick Wintour, *Web Providers to be Named and Shamed Over Offensive Conduct*, The Guardian, November 15, 2008 (full text available at: http://www.guardian.co.uk/technology/2008/nov/15/internet-children, last viewed on May 21, 2010).
[267] See generally FERTIK and THOMPSON, *supra* note 1, at 91 (describing these services).
[268] *id*.

way to enable them.[269] Additionally, anyone can comment on any search result, so there is no way for an Internet user to screen for true or false comments.[270] Google now also offers a Google Profile service that enables individuals to write a brief profile about themselves.[271] These profiles may be displayed at the bottom of Google search results for personal names.[272] However, this service is currently limited in its impact because of the placement of the profiles at the bottom of a page of search results where they may be missed by a searcher.[273] Additionally, they have limited use for people with common names.[274]

Another form of self-regulation which is potentially relevant to the protection of online reputation is the Wikipedia online dispute resolution service. It is more and more common for individuals to be profiled on Wikipedia which is a participatory and interactive repository for knowledge on many different subjects.[275] The participatory nature of Wikipedia means that an individual will not necessarily control information about her that may be posted on a Wikipedia page.[276] Wikipedia has its own online dispute resolution procedure to verify the accuracy of information posted, and this may be utilized by individuals harmed by false or decontextualized postings.[277] While this approach is specific to Wikipedia, there is no reason why other online service providers could not adopt similar approaches if they wanted to assist their users in combating reputational harms.

IV. Conclusions

"The Internet is a powerful and wonderful tool that has ushered in a new information age. If purposely misused, however, the internet can be terrifying, and even deadly."[278]

---

[269] *id.*

[270] *id*.

[271] *id*.

[272] *id.*

[273] *id*.

[274] *id*.

[275] *id*., at 182 ("Wikipedia … is a free collaboratively edited encyclopedia. Anyone can edit any article, and anyone can create new articles.")

[276] *id*. ("The vast majority of readers will find no relevant information about them on Wikipedia, but every now and then a malicious editor will slip an inappropriate reference or an unsubstantiated attack into the site.")

[277] *id*, at 182-183 (describing applications of Wikipedia's dispute resolution procedure to reputational injuries).

[278] Goodno, *supra* note 39, at 125.

The Internet is an unparalleled global communications medium. However, online interactions can be harmful, leading to emotional suffering and physical harm. The current legal system has gone some way towards protecting victims of online harms. However, the law still has a long way to go. Legal remedies will always suffer limitations related to time, cost, and jurisdictional challenges in a borderless online world. Further, the embarrassment and humiliation often associated with a victim bringing a complaint will chill much legal action.

Like many other aspects of Internet regulation, effective responses to online abuse will require a multi-modal regulatory framework. Regulatory modalities such as social norms, public education and market forces will need to interact to create more comprehensive responses to online abuses. Reputation management services play an important role in this regulatory matrix, but are subject to their own limitations. Current approaches to online abuse might be improved if the existing commercial services could be supplemented with more easily affordable pro bono services, and if individuals could be empowered themselves to engage proactively in reputation management strategies. Increased funding for, and use of, hotlines would also be a step forward both in combating specific abuses and in providing more reliable and comprehensive data about online abuses. Attempts at industry self regulation, potentially in concert with government incentives, would also be a useful development.

A number of the proposals made in this article would require funding which is always a tall order, particularly in troubled economic times. On a more positive note, most of the suggestions made here are not particularly difficult to implement. They predominantly take advantage of tools already available and apply them in new ways. The extra-legal remedies advocated here also have the advantage that they do not rely on government action other than potentially some funding, so they do not run into significant First Amendment concerns.[279] Additionally, enhancing private mechanisms avoids some of the problems typically inherent in litigating to identify and to assert jurisdiction over often anonymous or pseudonymous defendants. Tackling online abuses is a global problem. Private bodies acting in concert with each other and with domestic governments have a better chance of reaching optimum solutions than governments acting alone.

---

[279] For example, governments are generally permitted to fund programs that impact speech. See, for example, *United States v American Library Association*, 539 U.S. 194 (2003) (upholding a funding program that required libraries to filer Internet access as a conditioning of accepting government funding).