

# COMBATING CYBER-VICTIMIZATION

Jacqueline D. Lipton<sup>†</sup>

## TABLE OF CONTENTS

I.	<b>INTRODUCTION</b> .....	1104
II.	<b>CATEGORIZING ABUSIVE ONLINE CONDUCT</b> .....	1107
A.	DELINEATING THE BOUNDARIES OF ONLINE ABUSES.....	1107
1.	<i>Cyber-bullying</i> .....	1108
2.	<i>Cyber-harassment</i> .....	1110
3.	<i>Cyber-stalking</i> .....	1111
B.	COMPARING ONLINE AND OFFLINE ABUSES.....	1112
III.	<b>REDRESSING ONLINE WRONGS: GAPS IN THE EXISTING LEGAL FRAMEWORK</b> .....	1116
A.	CRIMINAL LAW.....	1117
1.	<i>Criminal Law Versus Civil Law</i> .....	1117
2.	<i>Federal Criminal Law</i> .....	1118
a)	Interstate Communications Act.....	1118
b)	Telephone Harassment Act.....	1118
c)	Interstate Stalking Punishment and Prevention Act.....	1119
d)	Computer Fraud and Abuse Act.....	1120
e)	Megan Meier Cyberbullying Prevention Act.....	1121
3.	<i>State Criminal Law</i> .....	1122
4.	<i>Suggestions for Drafting Effective Criminal Legislation</i> .....	1126

---

© 2011 Jacqueline D. Lipton, Ph.D.

† 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, Telephone: (216) 368-3303. The author would like to thank Professor Lyrrisa 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 University 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.

B.	TORT LAW .....	1129
1.	<i>Online Abuses: Common Challenges for Tort Law</i> .....	1129
2.	<i>Defamation</i> .....	1133
3.	<i>Privacy Torts</i> .....	1134
4.	<i>Intentional Infliction of Emotional Distress</i> .....	1137
C.	CIVIL RIGHTS LAW .....	1138
IV.	<b>EXTRA-LEGAL APPROACHES TO ONLINE WRONGS</b> .....	1139
A.	THE NEED FOR A MULTI-MODAL APPROACH.....	1140
B.	EMPOWERING VICTIMS TO COMBAT ONLINE ABUSES .....	1141
1.	<i>Reputation Management Techniques</i> .....	1141
2.	<i>Education</i> .....	1144
C.	A CRITIQUE OF EXISTING COMMERCIAL REPUTATION MANAGEMENT SERVICES.....	1145
D.	EFFECTIVE REPUTATION MANAGEMENT .....	1149
1.	<i>Enhanced Access to Reputation Management Services</i> .....	1149
2.	<i>Cyber-abuse Hotlines</i> .....	1150
3.	<i>Evolving Online Norms</i> .....	1151
4.	<i>Industry Self-Regulation</i> .....	1152
V.	<b>CONCLUSION</b> .....	1154

## I. INTRODUCTION

“Once, reputation was hard-earned and carefully guarded. Today, your reputation can be created or destroyed in just a few clicks.”<sup>1</sup>

Words can hurt. Whether true or false, whether spoken by friend or frenemy,<sup>2</sup> the cyber-pen is mightier than the sword.<sup>3</sup> In today’s networked society, abusive online conduct such as cyber-bullying and cyber-harassment can cause serious damage, including severe emotional distress,<sup>4</sup> loss of

---

1. MICHAEL FERTIK & 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.” *Frenemy Definition*, DICTIONARY.COM, <http://dictionary.reference.com/browse/frenemy> (last visited June 6, 2010).

3. See Raphael Cohen-Almagor, *Responsibility of Net Users*, in 2 *THE HANDBOOK OF GLOBAL COMMUNICATION AND MEDIA ETHICS* 415, 419 (Mark Fackler & Robert S. Fortner eds., 2011) (“Words can wound. Words can hurt. Words can move people to action.”).

4. See, e.g., Jacqueline Lipton, “*We, the Paparazzi*”: *Developing a Privacy Paradigm for Digital Video*, 95 IOWA L. REV. 919, 921–22 (2010) (discussing the “Star Wars Kid” incident in which a Canadian teenager filmed himself mimicking the use of a light saber, which prompted the creation of humiliating mash-up videos that resulted in him dropping out of school and requiring psychiatric care).

employment,<sup>5</sup> and even physical violence<sup>6</sup> or death.<sup>7</sup> Thirteen-year-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.<sup>8</sup> This is but one of an increasing number of examples of abusive online conduct.<sup>9</sup> Almost one in four teenagers reportedly experiences cyber-bullying,<sup>10</sup> and approximately sixty-five percent of children know someone who has been the victim of cyber-bullying.<sup>11</sup> Furthermore, a 2006 Pew Internet study found that one-third of online teenagers had been victims of online harassment and that thirty-nine percent of social network users have been cyber-bullied.<sup>12</sup> Online abuses—cyber-bullying, cyber-stalking, and cyber-harassment—

---

5. Danielle Keats Citron, *Cyber Civil Rights*, 89 B.U. L. REV. 61, 64 (2009) [hereinafter Citron, *Cyber Civil Rights*] (“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.”).

6. See, e.g., Danielle Keats Citron, *Law’s Expressive Value in Combating Cyber Gender Harassment*, 108 MICH. L. REV. 373, 396–97 (2009) [hereinafter Citron, *Harassment*] (“The online abuse inflicts significant economic, emotional, and physical harm on women in much the same way that workplace sexual harassment does.”); see also Kara Carnley-Murrhee, *Cyberbullying: Hot Air or Harmful Speech? Legislation Grapples with Preventing Cyberbullying Without Squelching Students’ Free Speech*, U. FLA. L. MAG., Winter 2010, at 17, 18 (describing the case of thirteen-year-old Hope Witsell, who committed suicide after being the victim of a “sexting” campaign—a variation of cyber-bullying in which sexually explicit images of the victim or sexually explicit messages about the victim are disseminated over digital communications services); *Cyber Bullies Target Girl*, BBC NEWS (May 24, 2003), [http://news.bbc.co.uk/2/hi/uk\\_news/england/nottinghamshire/2933894.stm](http://news.bbc.co.uk/2/hi/uk_news/england/nottinghamshire/2933894.stm) (“[The victim’s] family says there has been a two-year campaign of intimidation and she has twice been attacked in school.”).

7. Danielle Keats Citron, *Mainstreaming Privacy Torts*, 99 CALIF. L. REV. 1805, 1817 (2011) [hereinafter Citron, *Mainstreaming*] (“Today, the physical harm associated with information disclosures can become as serious as murder.”).

8. Gordon Tokumatsu & Jonathan Lloyd, *MySpace Case: “You’re the Kind of Boy a Girl Would Kill Herself Over,”* NBC LOS ANGELES (Jan. 26, 2009), <http://www.nbclosangeles.com/news/local-beat/Woman-Testifies-About-Final-Message-Sent-to-Teen.html> (describing the last electronic message sent by Megan Meier, the teenage victim of an infamous online cyber-bullying incident, before she committed suicide by hanging herself in her closet). See also Cohen-Almagor, *supra* note 3, at 421–24 (discussing the Meier incident); Lyrissa Barnett Lidsky, *Anonymity in Cyberspace: What Can We Learn from John Doe?*, 50 B.C. L. REV. 1373, 1386 (2009) (describing the Megan Meier incident and the legal responses to it).

9. For more examples of cyber-bullying conduct involving school-age children, see Drew Jackson, *Examples of Cyberbullying*, [http://www.slais.ubc.ca/courses/libr500/04-05-wt2/www/D\\_Jackson/examples.htm](http://www.slais.ubc.ca/courses/libr500/04-05-wt2/www/D_Jackson/examples.htm) (last updated Apr. 18, 2005); see also Citron, *Mainstreaming*, *supra* note 7, at 10–11 (giving examples of high-profile cases of online abuses).

10. Cohen-Almagor, *supra* note 3, at 423.

11. *Id.* at 22–23.

12. *Id.* at 23.

disproportionately affect “traditionally subordinated groups,”<sup>13</sup> which include women,<sup>14</sup> children,<sup>15</sup> and minorities.<sup>16</sup> The prevalence of this conduct suggests that more effective means are necessary to redress online wrongs and to protect victims’ reputations, but 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 tends to be time-consuming and expensive for victims. In the United States, many potential legal solutions will also face First Amendment hurdles.<sup>17</sup>

Unlike previous writing in this area, this Article considers legal solutions within a broader context, including alternative approaches to regulating online conduct such as public education and the more effective use of commercial reputation protection services. The Article makes specific suggestions for reform of tort and criminal laws, but more importantly it places the legal debate into a larger multi-modal framework aimed at 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. The principal issue addressed in this Article is how best to enable victims to combat harms and protect their own reputations. Part II explores the categories of abusive online conduct that require regulatory attention—cyber-bullying, cyber-harassment, and cyber-stalking—and contrasts these categories with their offline counterparts. Part III identifies gaps in the current law as applied to

---

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

14. Ann Bartow, *Internet Defamation as Profit Center: The Monetization of Online Harassment*, 32 HARV. J.L. & GENDER 383, 392 (2009) (citing Ellen Nakashima, *Sexual Threats Stifle Some Female Bloggers*, WASH. POST, Apr. 30, 2007, at A1) (explaining that “[a]s women gain visibility in the blogosphere, they are the targets of sexual harassment and threats” and tend to be “singled out in more starkly sexually threatening terms” than men, which is parallel to the treatment of women in chat rooms beginning in the early 1990s); *id.* at 394 (“Self-identifying as a woman online can substantially increase the risk of Internet harassment.”); *see* Citron, *Harassment*, *supra* note 6, at 378 (“While cyber attackers target men, more often their victims are female.”) (footnote omitted). But note that some victims of online harassment are men, such as male doctors. Citron, *Mainstreaming*, *supra* note 7, at 1817 (describing physical assaults and murders of doctors who perform abortions, where an online list of these doctors was involved in identifying them).

15. Citron, *Harassment*, *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.

17. For example, a number of laws directed at online speech have run afoul of the First Amendment. *See, e.g.*, *Ashcroft v. ACLU*, 542 U.S. 656 (2004) (invalidating content-regulating sections of the Child Online Protection Act); *Reno v. ACLU*, 521 U.S. 844 (1997) (invalidating content-regulating sections of the Communications Decency Act of 1996).

abusive online conduct, focusing on remedies found in criminal law, tort law, and, to a lesser extent, civil rights law. As part of this examination, it suggests ways in which current laws could be updated to more effectively combat online wrongs.

Part IV proposes extra-legal regulatory mechanisms that might better protect individual reputations online by surveying currently available options, such as commercial reputation management services,<sup>18</sup> and discussing their shortcomings. This Part advocates developing educational programs to empower victims of online abuses to utilize currently available legal and technological means for protecting their online reputations. Furthermore, 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 V concludes this Article by suggesting future directions in the regulation of online abuses, with a focus on extra-legal solutions. 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 internet service providers<sup>19</sup> play a more active role in monitoring and enforcing norms of accountability.

## II. CATEGORIZING ABUSIVE ONLINE CONDUCT

### A. DELINEATING THE BOUNDARIES OF 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.”<sup>20</sup>

Recent literature describes online abuse predominantly in terms of cyber-stalking, cyber-harassment, and cyber-bullying. However, none of these

---

18. *See, e.g.*, REPUTATION.COM, <http://www.reputationdefender.com/> (last visited Apr. 14, 2010); REPUTATION HAWK, <http://www.reputationhawk.com> (last visited June 6, 2010); UDILIGENCE, <http://www.udiligence.com> (last visited May 20, 2010) (service for student-athletes); YOUDILIGENCE, <http://www.youdiligence.com> (last visited May 20, 2010) (service for children).

19. Internet service providers include social networking sites such as Facebook and MySpace as well as other online services that enable people to connect with each other via digital devices.

20. FERTIK & THOMPSON, *supra* note 1, at 44.

terms has achieved a universally accepted definition, and there are significant areas of overlap between them. Some authors have coined umbrella terms such as cyber-victimization<sup>21</sup> and cyber-targeting<sup>22</sup> to encompass all of these categories of conduct. These commentators have avoided individual terms for different cyber-wrongs on the basis that overlaps between the classes of wrongs might “thwart clear analysis and the creation of successful solutions.”<sup>23</sup> 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.<sup>24</sup>

Nevertheless, a brief consideration of the kinds of conduct described in recent years as cyber-bullying, cyber-harassment, and cyber-stalking is a useful background to understanding cyber-victimization as a whole. 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 also necessary to understand the terms in order to appreciate the gaps in the current legal system that become apparent when pursuing a cyber-victimization case.

### 1. *Cyber-bullying*

“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.”<sup>25</sup>

The term cyber-bullying typically refers to online abuses involving juveniles or students.<sup>26</sup> While it is possible that in any given instance of cyber-

---

21. 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).

22. David A. Myers, *Defamation and the Quiescent Anarchy of the Internet: A Case Study of Cyber Targeting*, 110 PENN ST. L. REV. 667, 667–68 (2006).

23. Schwartz, *supra* note 21, at 409.

24. For example, 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, as threats are generally not protected speech. *See Planned Parenthood of the Columbia/Willamette, Inc. v. Am. Coal. of Life Activists*, 23 F. Supp. 2d 1182, 1188–89 (D. Or. 1998) (holding that threatening speech is not protected by the First Amendment); *see also* Cohen-Almagor, *supra* note 3, at 416.

25. FERTIK & THOMPSON, *supra* note 1, at 105.

26. Schwartz, *supra* note 21, at 410–11 (explaining that cyber-bullying, which has been described as the online counterpart to traditional playground bullying, usually refers both the victim and the victimizer as being minors or students, but can also encompass situations in which the culprit is a juvenile and the victim is an adult).

bullying at least one of the parties may not be a youth,<sup>27</sup> discussions about cyber-bullying generally revolve around school-age children and often call on schools to address the issue.<sup>28</sup> 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.”<sup>29</sup> It can involve tormenting, threatening, harassing, humiliating, embarrassing, or otherwise targeting a victim.<sup>30</sup>

In recent years, the term has also been increasingly used in the employment context to describe hostile or threatening conduct in the workplace.<sup>31</sup> 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, which is the typical focus of harassment laws.<sup>32</sup> Targets of workplace bullying are often perceived as a threat to the bully in some way.<sup>33</sup> This notion of

---

27. See, e.g., Tokumatsu & Lloyd, *supra* note 8 (reporting that the bully was the mother of a school mate of thirteen-year-old victim of cyber-bullying).

28. See, e.g., CAL. EDUC. CODE § 32261(d) (2009) (setting forth the legislative intent of fostering “interagency strategies, in-service training programs, and activities that will improve school attendance and reduce school crime[,] violence, . . . [and] bullying, *including bullying committed personally or by means of an electronic act*”) (emphasis added); Citron, *Harassment*, *supra* note 6, at 410 (“[P]arents 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.”); 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) (explaining that cyber-bullying typically involves “a child, preteen or teen [being] tormented, threatened, harassed, humiliated, embarrassed or otherwise targeted by another child, preteen or teen using the Internet, interactive and digital technologies, or mobile phones” but that adults can also be involved).

29. Henderson, *supra* note 28, at 381.

30. See *id.* (explaining that these types of behavior occur in the cyber-bullying context, but equally occur in face-to-face bullying).

31. See, e.g., *Bullies in the Office: Bullying Worse Than Sexual Harassment*, ABC NEWS, abcnews.go.com/index/playerindex?id=4527601 (last visited May 18, 2010); *Bullying: What Is It?*, BULLY ONLINE, <http://www.bullyonline.org/workbully/bully.htm#Why> (last visited May 20, 2010) (“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.”).

32. See FED. COMM’NS COMM’N (FCC), UNDERSTANDING WORKPLACE HARASSMENT, <http://www.fcc.gov/owd/understanding-harassment.html> (last updated Jan. 8, 2008) (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 . . .”).

33. *Bullying: What Is It?*, *supra* note 31, at 7 (“Jealousy (of relationships and perceived exclusion therefrom) and envy (of talents, abilities, circumstances or possessions) are strong motivators of bullying.”).

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, one of Meier’s classmates.<sup>34</sup> Drew targeted Meier because she was concerned that Meier was saying, or would say, unpleasant things about Drew’s daughter online, rather than because of Meier’s gender or race. Drew took on the false digital identity of a fictional young man “Josh Evans” in order to see what Meier might say about her classmates to a digital “friend.”

## 2. *Cyber-harassment*

Like harassment in the physical world, cyber-harassment should technically be limited to targeting people by virtue of their membership in a protected class such as race or gender.<sup>35</sup> 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,<sup>36</sup> which seems to cross the line between bullying and harassment. While it is directed at a protected class, mobbing is typical of bullying<sup>37</sup> and the aim of driving subjugated groups offline seems more about control than possession—typical characteristics of bullying as opposed to harassment.<sup>38</sup>

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 between classes of conduct may emerge that are more appropriate in the digital age than some of the existing distinctions. 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

---

34. See Cohen-Almagor, *supra* note 3, at 422 (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).

35. See FCC, *supra* note 32, at 1 (discussing workplace harassment).

36. Citron, *Cyber Civil Rights*, *supra* note 5, at 4 (discussing “the growth of anonymous online mobs that attack women, people of color, religious minorities, gays, and lesbians”).

37. See *Bullying: What Is It?*, *supra* note 31 (describing “gang” or “group” bullying, also known as “mobbing”).

38. Presentation, Erica Merritt, Workplace Bullying (Case Western Reserve Univ., May 18, 2010) (session notes and PowerPoint slides on file with author).

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.<sup>39</sup>

### 3. *Cyber-stalking*

Cyber-stalking involves conduct directed at a victim, rather than general communications about a victim. At least in some jurisdictions, cyber-stalking legislation requires a credible threat to the victim for there to be a violation of law.<sup>40</sup> Because some commentators have described cyber-stalking as a direct online analog to the offline crime of stalking, cyber-stalking may thus be defined as “the use of the Internet, e-mail, or other means of electronic communication to stalk or harass another individual.”<sup>41</sup> Similarly, stalking has typically been defined as involving “repeated harassing or threatening behavior.”<sup>42</sup> The goal of the traditional stalker is to exert control over a victim by instilling fear into her.<sup>43</sup> In the physical world, as in cyberspace, stalking can lead to actual physical harm.<sup>44</sup>

While cyber-bullying and cyber-harassment may damage an individual’s reputation or livelihood, cyber-stalking is more likely to result in severe and immediate emotional or physical harm. Thus, legislation aimed at redressing cyber-stalking may be able to stand up to First Amendment scrutiny more easily than legislation aimed at other kinds of online abuses.<sup>45</sup> While the First Amendment may protect the ability to say something unpleasant about another online—subject to defamation and privacy law—it is much less likely to protect the ability to send threatening e-mails.

---

39. For a fuller discussion of Congress’s attempts to pass regulations that do not violate the First Amendment, see *infra* Part III.

40. Schwartz, *supra* note 21, at 411 (“[O]ne commentator states that cyberstalking is distinct from cyberbullying because cyberstalking involves credible threats.”).

41. 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 & Richard Shafritz, *A Survey of Cyberstalking Legislation*, 32 UWLA L. REV. 323, 323 (2001).

42. See Goodno, *supra* note 41, at 128.

43. *Id.* at 127.

44. See *id.* at 128 (“[C]yberstalking involves repeated harassing or threatening behavior, which is often a prelude to more serious behavior.”); Citron, *Mainstreaming*, *supra* note 7, at 1817 (describing a case in which online stalking led to the murder of the victim by the stalker).

45. See Myers, *supra* note 22, at 675.

## B. COMPARING ONLINE AND OFFLINE ABUSES

“[T]hanks to the power of the Internet, attackers and gossipmongers enjoy instant global audiences and powerful anonymity.”<sup>46</sup>

Laws targeted at real world activities often do not translate well when applied to cyberspace. Despite facial similarities between physical abuses and cyber-abuses,<sup>47</sup> there are significant underlying differences. Cyber-attackers can utilize the Internet to harass their victims on a scale never before possible because of both the immediate effect of their conduct, and the speed and ease of the global dissemination of online information.<sup>48</sup> This immediate dissemination is inexpensive for the abuser and is not particularly time-consuming.<sup>49</sup> Online postings have a *constant* effect on the victim, as opposed to more transient conduct in the physical world.<sup>50</sup> Even where information about a victim is removed from one website, it may be cached and copied on other websites.<sup>51</sup> Online communications therefore have a permanent quality that real world conduct lacks.<sup>52</sup> Compounding the permanence effect is the fact that online information is easily searchable through Google and other popular search engines.<sup>53</sup> Thus, damaging information is more readily accessible to those who may be looking for it. It is also extremely difficult to redress problems relating to the availability of the damaging information. Attempts to publish corrective information may suffer from being uninteresting to many readers and thus may be de-

46. FERTIK & THOMPSON, *supra* note 1, at 6.

47. Goodno, *supra* note 41, at 128 (discussing the similarities of cyber-stalking with offline stalking as being “a desire to exert control over the victim; and . . . repeated harassing or threatening behavior, which is often a prelude to more serious behavior”).

48. *Id.* at 128–29.

49. *Id.* at 129.

50. *Id.*; Citron, *Mainstreaming*, *supra* note 7, at 1813 (“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.”).

51. FERTIK & THOMPSON, *supra* note 1, at 54–55 (discussing the impact of the Internet Archive on the permanent quality of online information); Citron, *Mainstreaming*, *supra* note 7, at 1813; Lipton, *supra* note 4, at 977 (“[W]ith 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.”).

52. Citron, *Mainstreaming*, *supra* note 7, at 1813.

53. FERTIK & THOMPSON, *supra* note 1, at 53–54 (illuminating the fact that conversations and notes among friends were formerly more private and lacked permanence, “[b]ut 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”).

prioritized in search results when search engines are designed to focus on popularity of information. Blogs also tend to list comments in order of posting, thus making a rebuttal comment by a victim difficult to find as compared with the original damaging posting.

A cyber-attacker can also be physically removed from the victim. He may be across the state, across the country, or even across the globe.<sup>54</sup> The unlimited reach of the Internet differentiates online abuse from its offline counterparts in three important respects. First, online abusers can initiate and pursue their wrongful act inexpensively and easily from anywhere in the world.<sup>55</sup> 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 at some far away location.<sup>56</sup> 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.<sup>57</sup>

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 computer and walking away. However, in today's interconnected world that is not a viable option, as people who are forced offline forgo important personal and professional opportunities.<sup>58</sup> Also, if a victim moves offline, this 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 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

---

54. FERTIK & 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.”); Goodno, *supra* note 41, at 129 (“Cyberstalkers can be physically far removed from their victim.”).

55. Goodno, *supra* note 41, at 129.

56. *Id.*

57. *Id.* at 129–30; *see infra* Section II.B.

58. MARY MADDEN & AARON SMITH, PEW RESEARCH CTR., REPUTATION MANAGEMENT AND SOCIAL MEDIA: HOW PEOPLE MONITOR THEIR IDENTITY AND SEARCH FOR OTHERS ONLINE 3 (2010) (“12% of employed adults say they need to market themselves online as part of their job.”); Citron, *Harassment*, *supra* note 6, at 398 (explaining that women who are victims of cyber-victimization miss out on opportunities if they choose to “close their blogs, disengage from online communities, and assume pseudonyms”).

physical contact, the opposite may be true.<sup>59</sup> 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<sup>60</sup>—people are less inhibited when faced with a computer terminal than when faced with a live person.<sup>61</sup> Cyberspace also enables perpetrators of online abuses to spy on their victims in virtual space for extended periods of time without ever being detected.<sup>62</sup> Furthermore, anonymity naturally makes it more difficult for victims and law enforcement officers to identify and locate cyber-wrongdoers.<sup>63</sup>

Cyberspace also enables perpetrators to manipulate the victim's identity online.<sup>64</sup> Cyber-abusers can both impersonate their victims and can manipulate others' reactions to their victims.<sup>65</sup> They may pretend to be their victims and send inflammatory messages to online discussion groups or social networks under the guise of the victim.<sup>66</sup> Wrongdoers may also engage in identity theft for financial purposes.<sup>67</sup> Additionally, retaliation against the

---

59. *See generally* Schwartz, *supra* note 21, at 412, 414–15.

60. *Id.* at 414–15.

61. *See* FERTIK & THOMPSON, *supra* note 1, at 76–78 (describing psychological studies and theories on dis-inhibition effects when perpetrators of harm are physically removed from their victims); Cohen-Almagor, *supra* note 3, at 418 (“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, *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.”); Lyriisa Barnett Lidsky & Thomas Cotter, *Authorship, Audiences, and Anonymous Speech*, 82 NOTRE DAME L. REV. 1537, 1575 (2007) (“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.”); Schwartz, *supra* note 21, at 414–15 (“[A]nonymity makes it easier for the perpetrator to overcome person inhibitions that might have deterred him from carrying out the victimizing behavior if he were confronting his victim face-to-face.”).

62. *See generally* Schwartz, *supra* note 21, at 415–16.

63. Goodno, *supra* note 41, at 131.

64. FERTIK & THOMPSON, *supra* note 1, at 78–79 (explaining that such “[a]ttacks 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?”).

65. *See* Schwartz, *supra* note 21, at 413–16.

66. *Id.* at 1815.

67. Citron, *Mainstreaming*, *supra* note 7, at 1817–18 (“Identity thieves use SSNs and biometric data [obtained through data leaks] to empty bank accounts, exhaust others’ credit card limits, secure loans, and flip property,” which may cause the victim to “face financial ruin.”).

victim often follows. It 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.<sup>68</sup>

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. 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.<sup>69</sup> 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.<sup>70</sup>

In practice, it is very difficult for victims of these kinds of impersonation attacks to effectively fight back. Because identities are extremely difficult to verify online, it can be almost impossible for a victim to establish that she was not in fact the person who posted the comments in question.<sup>71</sup> It is very difficult for the victim to prove a negative; that is, the "I didn't do it" part of the equation.<sup>72</sup> Even if she can, the victim's revocation may attract more attention to the original content and ultimately make the damage worse.<sup>73</sup> 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

---

68. *Id.*

69. *Id.*

70. *Id.*

71. See FERTIK & THOMPSON, *supra* note 1, at 78–79 (noting the difficulty of showing that it was the abuser, not the victim, who made the online comments).

72. *Id.*

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

it.<sup>74</sup> As noted by the founder and the general counsel of ReputationDefender, “many victims feel completely helpless when faced with an anonymous impersonator.”<sup>75</sup>

Overall, while online attackers will engage in a variety of damaging types of conduct—harassment, bullying, and stalking—the conduct will have different effects online than its analogs in the physical world. The reputation-damaging information will have a permanent and global quality, and rebuttals by the victim may be difficult to find in practice. Much online conduct will damage a victim’s reputation permanently with little recourse because many laws are focused on physical world conduct rather than online communications. The resulting limitations of legal solutions are considered in the following Part.

### III. REDRESSING ONLINE WRONGS: GAPS IN THE EXISTING LEGAL FRAMEWORK

This Part examines the currently existing matrix of state and federal laws, both civil and criminal, that potentially could be applied to the kinds of conduct described in this Article. It identifies serious limitations with these laws, particularly those existing in federal criminal laws. While some of these limitations could potentially be redressed through legislative amendments to bring laws into the digital age, many of the limitations do not have feasible legislated solutions. As noted in the Introduction, law alone cannot be the sole answer to problems of cyber-victimization, as laws have jurisdictional and First Amendment limitations. This is not to say that the law should not be an important part of the regulatory matrix aimed at protecting victims against cyber-victimization. However, those making and enforcing laws should be aware of the limitations of legal solutions and should ensure that laws work in tandem with non-legal solutions, such as public education about self-protection online. Furthermore, laws also serve an important expressive function about acceptable modes of online behavior even in situations where their enforcement may be limited by a variety of the factors discussed below.

---

74. *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.”).

75. *Id.*

## 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 on the public judicial record the humiliation, embarrassment, shame, and fear attached to the defendant's conduct.<sup>76</sup> Therefore, closed criminal trials may be preferable in particularly sensitive cases.<sup>77</sup> However, closed criminal trials raise constitutionality concerns and have been difficult to achieve in practice in other contexts. In addition, absent effective privacy protections, victims of online abuses may be reticent to make complaints or to give evidence in court.<sup>78</sup>

Unlike civil law, criminal law does not typically require a victim to shoulder the costs of a lawyer 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 related online conduct to make a credible case against the abuser.<sup>79</sup> The current lack of reliable data on the prevalence of cyber-stalking, for example, might be attributable to both the failure of victims to bring complaints and the lack of adequate training and funding for police and prosecutors to effectively deal with online abuses.<sup>80</sup>

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.<sup>81</sup> Where the concern is with deterring and punishing aberrant conduct, criminal law will be an important part of the regulatory matrix.

---

76. Lipton, *supra* note 4, at 961.

77. *See, e.g.*, Press Enter. Co. v. Super. Ct. of Cal., 478 U.S. 1 (1986) (reversing the order sealing the transcript of lower court proceedings on First Amendment grounds).

78. *See id.* at 3.

79. FERTIK & THOMPSON, *supra* note 1, at 6 (“Many victims of ‘routine’ online attacks cannot obtain help from the legal system . . . 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.”); Citron, *Harassment*, *supra* note 6, at 402–03 (“[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.”).

80. *See* Goodno, *supra* note 41, at 156 (discussing the fact that few government officials have had training in cyber-stalking issues).

81. Schwartz, *supra* note 21, at 427 (“[C]yber 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.”).

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 federal and state criminal laws identifies existing gaps in these laws in the online context and makes suggestions for reform.

## 2. *Federal Criminal Law*

### a) Interstate Communications Act

Federal legislation contains many gaps and inconsistencies when applied to online abuses.<sup>82</sup> 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 “[w]hoever 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.”<sup>83</sup> This provision has limited application to online abuses because of its requirement of a threat of physical injury,<sup>84</sup> as 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.<sup>85</sup> 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. Thus, this legislation will have limited application to the types of cyber-victimization on which this Article focuses.

### b) Telephone Harassment Act

Alternatively, the federal Telephone Harassment Act may have relevant applications to cyber-wrongs. 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.”<sup>86</sup> The revisions to the statute were intended to capture

---

82. Carnley-Murree, *supra* note 6, at 18 (describing federal legislation in the cyber-bullying area as being a “void”).

83. 18 U.S.C. § 875(c) (2006).

84. Goodno, *supra* note 41, at 147–48; *see* United States v. Alkhabaz, 48 F.3d 1220 (6th Cir. 1995) (mentioning that an actual threat must be directed to the recipient of the communication).

85. Goodno, *supra* note 41, at 147–48.

86. 47 U.S.C. § 223(a)(1)(C) (2006).

harassing e-mails.<sup>87</sup> While the provision will cover some cyberspace abuses, particularly the sending of threatening or harassing e-mails, it has some limitations. For example, it is limited to acts “in interstate or foreign communications,”<sup>88</sup> but 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 law will not apply to situations in which a perpetrator simply posts information about the victim on a website, or where he poses as the victim.<sup>89</sup> Another limitation of the statute is that it carves out situations where the perpetrator has not remained anonymous.<sup>90</sup> In order for the prohibition to apply, the perpetrator must have failed to disclose his identity and the victim cannot otherwise have gained knowledge of his identity.<sup>91</sup> Again, this statute is unlikely to have significant application in situations involving the kinds of cyber-abuses under discussion in this Article.

### 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” 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.”<sup>92</sup> 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

---

87. Goodno, *supra* note 41, at 148–49.

88. 47 U.S.C. § 223(a)(1).

89. Goodno, *supra* note 41, at 150 (stating that because the Telephone Harassment Statute “applies only to direct communications between the stalker and victim, . . . the amended statute is inadequate to deal with behavior where the cyberstalker indirectly harasses or terrorizes his victim”).

90. *Id.* (“It seems odd to only make cyberstalking a crime where the identity of the cyberstalker is unknown [as this] carves out a number of terrifying cases where the victim knows the identity of the cyberstalker.”).

91. Lidsky & Cotter, *supra* note 61, at 1590 (explaining 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).

92. 18 U.S.C. § 2261A(1), (2) (2006).

to a victim. The FISPPA instead focuses 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.<sup>93</sup> In addition, unlike the Telephone Harassment Act, the FISPPA will apply where the defendant is not anonymous.<sup>94</sup> 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. Therefore, the FISPPA will similarly be far from a comprehensive answer to cyber-victimization problems.

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).<sup>95</sup> This legislation was originally aimed at unauthorized hacking into computer systems and was not focused on personal attacks. However, prosecutors in *Drew* creatively utilized the CFAA to bring criminal proceedings against Drew, who had perpetrated a cyber-bullying attack resulting in the suicide of thirteen-year-old Meier.<sup>96</sup> 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.<sup>97</sup> Evans never really existed but was rather 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.<sup>98</sup>

---

93. Goodno, *supra* note 41, 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.’”).

94. *Id.* (“[The FISPPA does not] limit coverage of the ‘use’ of the computer to only anonymous e-mail messages.”).

95. 18 U.S.C. § 1030 (2006).

96. *United States v. Drew*, 259 F.R.D. 449 (C.D. Cal. 2009); Henderson, *supra* note 28, at 393 (explaining that, despite Drew’s egregious acts, only through “creatively interpreting the federal Computer Fraud and Abuse Act [were] federal officials [able to] charge[] her with conspiracy and unauthorized access of a computer”); Lidsky, *supra* note 8, at 1386 (describing the legal action in the Lori Drew case).

97. Henderson, *supra* note 28, at 379.

98. *Id.* at 379–80.

Drew's conduct was not a criminal act under local Missouri law.<sup>99</sup> 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.<sup>100</sup> During the initial trial, a jury found that Drew had infringed provisions of the CFAA relating to making unauthorized access to, or exceeding authorized access to, a computer.<sup>101</sup> However, on appeal, a motion by Drew to acquit and overturn the misdemeanor conviction was granted.<sup>102</sup> 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.<sup>103</sup> Thus, Drew's misuse of the MySpace website could not result in criminal liability under the CFAA. This is not a surprising outcome because, as with the other federal laws discussed in this Section, the CFAA was not enacted specifically to deal with cyber-victimization of this kind.

e) Megan Meier Cyberbullying Prevention Act

In the wake of the Meier incident, federal legislation was proposed that would be more clearly directed at cyber-bullying than any existing federal laws. The Megan Meier Cyberbullying Prevention Act<sup>104</sup> was introduced in 2008 but was 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; using electronic means to support severe, repeated, and hostile behavior."<sup>105</sup> The definitions of "communication" and "electronic means" in the bill were fairly

---

99. *Id.* at 380.

100. *Id.* at 393.

101. *Drew*, 259 F.R.D. at 453 ("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.'") (internal alterations omitted).

102. *Id.* at 468.

103. *Id.* at 464 (holding that basing a CFAA violation on a terms of service agreement runs afoul of the void-for-vagueness doctrine not only "because of the absence of minimal guidelines to govern law enforcement, but also because of actual notice deficiencies"); *id.* at 467 (explaining that a contrary result would "afford[] too much discretion to the police and too little notice to citizens who wish to use the [Internet]").

104. H.R. 6123, 110th Cong. (2d Sess. 2008).

105. *Id.* § 3(a).

broad and would have encompassed modern Web 2.0 technologies such as blogs and online social networks.<sup>106</sup>

While this legislation would have been broad enough to cover much abusive online conduct, it is arguably overbroad for a variety of reasons. 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.<sup>107</sup> Additionally, while aimed at the Meier incident and drafted with a view to protecting minors,<sup>108</sup> the text of the statute is not expressly limited to conduct involving minors. As a result, the bill may have been unconstitutional on First Amendment grounds because it may have inadvertently sanctioned constitutionally protected expression among adults.<sup>109</sup>

This survey of federal criminal legislation that might potentially apply to cyber-victimization evidences the fact that there are currently no federal laws that are aimed clearly at cyber-victimization. The pastiche of laws that may incidentally catch aspects of cyber-victimization is problematic in practice. The lack of clear federal legislation may not be so much of a problem if there were a series of harmonized state laws that dealt with the issue of cyber-victimization. However, as the following discussion demonstrates, state criminal laws are disharmonized and many have not been brought up to date to deal with challenges posed by the digital age and online social networking technologies.

### 3. *State Criminal Law*

One state criminal law that has been particularly well-developed with respect to cyber-victimization is the Missouri statute dealing with online and offline harassment. This law was updated in the wake of the Meier incident

---

106. *Id.* § 3(b).

107. 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 . . .”).

108. H.R. 6123 § 2 (contemplating that the purpose of the bill is to protect children aged from two to seventeen years old).

109. In the past, legislatures have had difficulty establishing that laws abridging online speech are sufficiently narrowly tailored to survive First Amendment scrutiny. *See, e.g.,* *Ashcroft v. ACLU*, 542 U.S. 656, 665, 670 (2004) (holding that a statute that imposed criminal penalties for posting content harmful to minors on the Internet was unconstitutional under the First Amendment); *Reno v. ACLU*, 521 U.S. 844, 849 (1997) (holding that a statute attempting to restrict minors’ access to harmful material was unconstitutional under the First Amendment).

to ensure that online bullying would be effectively 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 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.<sup>110</sup>

This statute is a good model for legislating against abusive online conduct because it covers multiple communications media, including the Internet, and 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,<sup>111</sup> the final sub-section does not require a communication directed to the victim.<sup>112</sup> 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.<sup>113</sup>

The statute 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.<sup>114</sup> This may be a factor that courts should consider in applying

---

110. MO. REV. STAT. § 565.090(1) (2011).

111. § 565.090(1)(3), (4).

112. § 565.090(1)(6).

113. *Id.*

114. SUTTON, *supra* note 107, at 11.

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. Because of this, courts applying the statute may need to consider whether the defendant’s speech should be protected on constitutional grounds.

In recent years a number of other states have also enacted laws targeted specifically at online conduct.<sup>115</sup> However, most states still rely on pre-Internet legislation.<sup>116</sup> Nebraska, for example, maintains stalking and harassment legislation that does not expressly contemplate electronic conduct. The Nebraska Revised Code states that “[a]ny person who willfully harasses another person . . . with the intent to injure, terrify, threaten, or intimidate commits the offense of stalking.”<sup>117</sup> 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.”<sup>118</sup> “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.”<sup>119</sup>

This legislative approach fails to cover a number of prominent 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. 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, because 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, but legislators updated the New Jersey statute in 2009. The new statute defines “course of conduct” as:

---

115. Carnley-Murrhee, *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 within state boundaries . . .”).

116. *Id.*

117. NEB. REV. STAT. § 28-311.03 (2010).

118. *Id.* § 28-311.02(2)(a).

119. § 28-311.02(2)(b).

[R]epeatedly 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.<sup>120</sup>

Unlike Nebraska's law, the New Jersey statute covers 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 to be raped and providing her personal contact details.<sup>121</sup>

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. For example, Florida's relatively new cyber-stalking legislation defines cyber-stalking 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

---

120. N.J. REV. STAT. § 2C:12-10(a)(1) (2010).

121. Citron, *Mainstreaming*, *supra* note 7, at 1839 n.266.

legitimate purpose.”<sup>122</sup> 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*.<sup>123</sup> It is at least arguable that posting damaging information *about* an individual is not the same as directing that communication *to* the individual in question. Thus, while the New Jersey statute may cover these kinds of scenarios, the Floridian statute may well not extend this far. The differences in drafting between the criminal laws in different states also cause significant lack of harmonization where abusive online conduct crosses state borders.

#### 4. *Suggestions for 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.<sup>124</sup> On the other hand, legislators may want to retain some laws with a credible 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.<sup>125</sup>

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

---

122. FLA. STAT. § 748.048(1)(d) (2009).

123. See Goodno, *supra* note 41, 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.”); *id.* at 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.”).

124. *Id.* at 136 (“In cyberstalking cases, a statute with a credible threat requirement does not protect against electronic communications (such as thousands of e-mail messages) that are harassing, but do not include an actual threat.”); *id.* at 138 (listing problems of a credible threat requirement as including proof of receipt by the victim, as “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;” and the “require[ment] the victim to prove that the cyberstalker had the ‘apparent ability’ to carry out whatever he threatens, . . . [which] is onerous and unnecessary”); Schwartz, *supra* note 21, at 429 (“[N]one of the crimes should require an element of proximity to the victim, nor should they include an ‘overt’ or ‘credible’ threat requirement.”).

125. See discussion *infra* Part IV.

threaten or harass another.<sup>126</sup> 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.<sup>127</sup> 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, determining 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 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.

Criminal legislation aimed at online abuses should also maintain the mens rea requirements that currently exist in state legislation. For example, the Nebraska statute requires willful conduct on the part of the perpetrator.<sup>128</sup> Such a willfulness requirement may go some way towards mitigating any perceived harshness inherent in allowing judges to sanction one-time abuses.

Effective legislation should not require a communication to be sent directly to the victim.<sup>129</sup> 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

---

126. SUTTON, *supra* note 107, at 11; Schwartz, *supra* note 21, at 430 (emphasizing the importance of a requirement of repetitive conduct).

127. Citron, *Mainstreaming*, *supra* note 7, at 1813 (describing the permanence of information posted online); Lipton, *supra* note 4, at 977 (describing the use of internet archives to maintain permanent records of information posted online).

128. 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.”). *See supra* Section III.A.3.

129. *See* Goodno, *supra* note 41, at 146 (noting problems with current anti-cyber-stalking statutes in Louisiana and North Carolina in that those statutes require harassing communications to be sent “to another”).

of “Facebook friends.”<sup>130</sup> 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. The First Amendment protects the right to speak freely and also the right for others to receive speech against government intrusion. Thus, legislation that restricts communication can be problematic, particularly where the information communicated is not in a class of speech that the government has traditionally been able to restrict in certain cases, such as protecting children from pornography or protecting individuals’ reputations from false and defamatory statements.

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.<sup>131</sup> 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.<sup>132</sup> 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 a reasonable person standard relating to the victim’s state of mind.<sup>133</sup> 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

---

130. Lipton, *supra* note 4, at 939–40 (describing the concept of “Facebook friends”).

131. Schwartz, *supra* note 21, at 431–32; *see* FLA. STAT. § 784.048(1)(b) (2008) (“‘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 protected activity is not included within the meaning of ‘course of conduct.’”); § 748.048(1)(d) (“‘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.”).

132. *See* statutes discussed *supra* Section II.A.2.

133. Goodno, *supra* note 41, at 139–40 (“Those stalking statutes that have a reasonable person standard provide the most successful way to prosecute cyberstalking . . . [because] the standard focuses on the victim and whether it is reasonable for her to fear for her safety because of the cyberstalker’s conduct.”).

that involves 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.<sup>134</sup> 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 could incite tort-based lawsuits, including defamation,<sup>135</sup> privacy torts,<sup>136</sup> and intentional infliction of emotional distress.<sup>137</sup> As with the federal criminal laws discussed above, many tort laws have not been developed specifically to address the kinds of cyber-abuses under consideration in this Article. Defamation and privacy torts are good examples. 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.<sup>138</sup> While it is possible to unmask anonymous actors online,<sup>139</sup> often much

---

134. See MO. REV. STAT. § 565.090(1) (2011); see discussion *supra* Section II.A.3.

135. Kara Carnley-Murrhee, *Sticks & Stones: When Online Anonymous Speech Turns Ugly*, U. FLA. L. MAG., Winter 2010, at 21, 22 (citing Lyrissa Lidsky describing the ease of bringing defamation actions for objectionable speech online); Citron, *Cyber Civil Rights*, *supra* note 5, at 87–88 (“Targeted individuals [of online 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 John Doe: Defamation and Discourse in Cyberspace*, 49 DUKE L.J. 855, 888–92 (2000) (expressing concerns that defamation suits will be the obvious type of legal action to combat online abuses and such suits may stifle online discourse).

136. Carnley-Murrhee, *supra* note 6, at 19 (citing Scott Bauries, who notes that tort actions for invasion of privacy might be a useful approach to cyber-bullying).

137. Citron, *Cyber Civil Rights*, *supra* note 5, at 88 (“Many victims [of online abuses] may have actions for intentional infliction of emotional distress.”); Lyrissa Lidsky, Comment to *New Cyberbullying Case: D.C. v R.R.*, PRAWFSBLAWG (Mar. 18, 2010, 3:45 PM), <http://prawfsblawg.blogs.com/prawfsblawg/2010/03/new-cyberbullying-case-dc-v-rr.html#comments> (noting that intentional infliction of emotional distress is relevant to new cyber-bullying case).

138. For example, this problem includes the TOR anonymizing software. See *Tor: Overview*, TORPROJECT, <http://www.torproject.org/overview.html.en> (last visited April 14, 2010) (“Individuals use TOR to keep websites from tracking them . . . .”); see also FERTIK & THOMPSON, *supra* note 1, at 71 (discussing anonymizing technologies, including TOR).

139. For some examples of “unmasking” litigation, see *In re Verizon Internet Services*, 257 F. Supp. 2d 244 (D.D.C. 2003) (attempting to unmask anonymous online copyright infringers under subpoena provisions in 17 U.S.C. § 512); *Columbia Ins. Co. v. Seescandy.com*, 185 F.R.D. 573 (N.D. Cal. 1999) (attempting to identify anonymous domain

damage has been done by the time the actor is identified.<sup>140</sup> In addition, unmasking a perpetrator of an online abuse may require a court order.<sup>141</sup> This can be expensive and time consuming, outside the budget of many victims of cyber-abuses.<sup>142</sup> Additionally, as with any litigation, the judicial proceedings potentially bring more publicity to the situation. Non-legal approaches to reputation protection, on the other hand, may be superior in many circumstances involving cyber-victimization because they avoid this level of publicity. These non-legal approaches are discussed in more detail in the next Part.

Another practical problem hypothetically 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 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 potential 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. Any legal action used to identify anonymous speakers thus 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.<sup>143</sup> Many of the extra-legal approaches to

---

name cyber-squatter); *In re Subpoena Duces Tecum to Am. Online*, 52 Va. Cir. 26 (2000) (attempting to unmask anonymous online defendants).

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

141. *See Doe I v. Individuals, Whose True Names Are Unknown*, 561 F. Supp. 2d 249 (D. Conn. 2008) (seeking to identify anonymous posters on AutoAdmit bulletin board in order to proceed with civil action relating to a number of torts dealing with reputational harm caused to the plaintiffs); *In re Subpoena Duces Tecum*, 52 Va. Cir. 26 (prospective plaintiff sought a court order to unmask identifies of AOL subscribers so that they could be named as defendants in an action for defamation).

142. Lidsky, *supra* note 8, at 1387 (noting that many victims of online defamation lack the resources to bring suit).

143. Bartow, *supra* note 14, at 386–87 (clarifying that the students in the *AutoAdmit* case were first victimized by people they knew in real life, “[b]ut 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”); *id.* at 399 (“The AutoAdmit administrators seemed to intentionally create a climate that encouraged angry, widespread flaming of anyone who complained about the way they were treated by posters at the AutoAdmit boards.”).

protecting online reputations discussed in Part IV 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.<sup>144</sup> Along with these burdens, a victim would have to relive the shame and humiliation of the abuse during the proceedings, which occur on the public record.<sup>145</sup> 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, he 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,<sup>146</sup> 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. Additionally, many individual defendants may well be impecunious and, therefore, effectively judgment-proof. In any event, the plaintiff's desired remedy will often not be damages, but rather an injunction to remove a harmful online posting. Some online communications services, such as many common blogs, will not give the original comment poster the technical access to remove the harmful posting.

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).<sup>147</sup> Section

---

144. *Id.*; Citron, *Cyber Civil Rights*, *supra* note 5, at 91 (noting that many plaintiffs in the cyber-harassment context cannot afford the high costs of litigation); Schwartz, *supra* note 21, at 427 (highlighting, through the perspective a victim of cyber-victimization, how the costs and difficulties of litigation deter victims from seeking civil redress).

145. Lidsky, *supra* note 8, at 1390 (“[S]uing often brings more attention to libelous statements.”); Lipton, *supra* note 4, at 961 (noting that as part of the court proceedings, 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).

146. Lidsky, *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).

147. 47 U.S.C. § 230(c)(1) (2000) (“No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider.”).

230 immunizes providers and users of “interactive computer services” from liability for information “provided by another information content provider.”<sup>148</sup> 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.<sup>149</sup>

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 courts.<sup>150</sup> For victims, online service providers are the most effective points in the chain of communications for victims to pursue. In general, the platforms provide the gateways for online discourse, allow victims of online abuses to easily identify them, possess the financial resources to compensate victims by way of damages, and 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.<sup>151</sup> Further, the near-absolute immunity<sup>152</sup> of online service providers under § 230 has in practice prevented courts from engaging in meaningful discussions about the standard of care that might be expected

---

148. *Id.*

149. FERTIK & 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.”); Citron, *Mainstreaming*, *supra* note 7, at 1839 (“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.”).

150. *See, e.g.*, *Zeran v. Am. Online, Inc.*, 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 on the basis 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).

151. *See Blumenthal*, 992 F. Supp. at 51–52.

152. Internet service provider immunity 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*, *supra* note 7, at 1839 (“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.”).

of these service providers absent the statutory immunity.<sup>153</sup> While § 230 immunizes intermediaries and disincentivizes them from monitoring online postings, a victim may effectively have no legal remedy 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.<sup>154</sup>

## 2. Defamation

Defamation law only protects victims against false statements<sup>155</sup> that harm their reputations.<sup>156</sup> Many online statements are true, even if unpleasant or embarrassing. Many are also statements of opinion, which are not typically actionable.<sup>157</sup> Even where the comments are true, the victim 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 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.<sup>158</sup> Thus, even the possibility of a small

---

153. Citron, *Cyber Civil Rights*, *supra* note 5, at 117 (citing “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”).

154. FERTIK & 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.”).

155. RESTATEMENT (SECOND) OF TORTS § 558(a) (1977) (requiring a “false and defamatory statement” as an element of a defamation action).

156. *Id.* § 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.”).

157. *Id.* § 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, *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.”).

158. NEIL NETANEL, COPYRIGHT’S PARADOX, 104–05 (2008) (describing how laws often serve “an expressive or symbolic function above and beyond regulating or providing incentives for conduct. . . . 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”); Lidsky, *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).

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.

### 3. *Privacy Torts*

The American privacy torts were developed at a time well before the age of electronic communications technologies.<sup>159</sup> The laws are focused largely on reasonable expectations of privacy drawn from paradigms involving physical space.<sup>160</sup> 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 her 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.<sup>161</sup> These torts are: (a) intrusion into seclusion;<sup>162</sup> (b) public disclosure of private facts;<sup>163</sup> (c) false light publicity;<sup>164</sup> and (d) commercial

---

159. Citron, *Mainstreaming*, *supra* note 7, at 1807 (“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.”).

160. Patricia Sánchez Abril, *Recasting Privacy Torts in a Spaceless World*, 21 HARV. J.L. & TECH. 1, 2 (2007) (“[P]rivacy is usually a function of the physical space in which the purportedly private activity occurred . . . .”); *id.* at 3 (“Traditionally, privacy has been inextricably linked to physical space.”).

161. William Prosser, *Privacy*, 48 CALIF. L. REV. 383 (1960).

162. RESTATEMENT (SECOND) OF TORTS § 652B (1977) (“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.”).

163. *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.”).

164. *Id.* § 652E (making a person liable for false light when “(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”).

misappropriation of name or likeness.<sup>165</sup> None of these torts are obvious matches 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.<sup>166</sup> 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.<sup>167</sup>

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,<sup>168</sup> there is as yet no judicial authority on point.<sup>169</sup> Another potential limitation of the intrusion tort, even if it were extended to online conduct, is that it would likely apply only 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 some 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."<sup>170</sup> 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

---

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

166. Citron, *Mainstreaming*, *supra* note 7, at 1828 ("[P]laintiffs cannot bring intrusion on seclusion claims . . . because online postings do not involve invasions of a place or information that society recognizes as private.").

167. *Id.*

168. Citron, *Cyber Civil Rights*, *supra* note 5, at 89 ("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.").

169. 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 89 n.204 (citing *Donnel v. Lara*, 703 S.W.2d 257, 260 (Tex. Ct. App. 1985)).

170. *Id.* at 89 (citing RESTATEMENT (SECOND) OF TORTS § 652B (1977)).

significant burden on plaintiffs to prove offense.<sup>171</sup> 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.<sup>172</sup> 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 be applicable to online harassment because this tort requires the defendant to have made an unauthorized commercial profit from the plaintiff's name or likeness.<sup>173</sup> Most online abuse is non-commercial. It is possible that a plaintiff might bring an appropriation action against the operator of a web service that made money from encouraging personally hostile discourse. For example, a service like AutoAdmit or Juicy Campus<sup>174</sup>—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 instead provided a forum for others to appropriate names and

---

171. Lipton, *supra* note 4, at 932 (“The [public disclosure tort] also generally requires that the private facts in question be shameful by an objective standard that is often difficult to prove.”); Jonathan B. Mintz, *The Remains of Privacy's Disclosure Tort: An Exploration of the Private Domain*, 55 MD. L. REV. 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.”).

172. See Citron, *Mainstreaming*, *supra* note 7, at 1827 (“False light claims require proof of a plaintiff's placement in a false light. [They] do not apply when . . . leaked information causes mischief because it is true.”).

173. RESTATEMENT (SECOND) OF TORTS § 652C (1977) (“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.”).

174. Cohen-Almagor, *supra* note 3, at 418–420 (discussing the moral responsibility of services like Juicy Campus for harmful postings by their members). These services typically post gossip amongst college students and much of the gossip is extremely hurtful.

likenesses for abusive discourse and has profited from providing that forum, a court may hold that the elements of the tort are not satisfied.<sup>175</sup> 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.<sup>176</sup> 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.<sup>177</sup> 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.<sup>178</sup>

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 cyber-bullying and cyber-harassment will have powerful emotional effects on their victims. For example, a recent online posting on the “Casual Encounters” board on Craigslist said that a teenager had rape fantasies and enjoyed pornography. As a result of the posting, the teenager was inundated with pornographic messages and confronted by men at her work.<sup>179</sup> 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, and potential increased public humiliation for either or both parties.

---

175. *But see* Citron, *Mainstreaming*, *supra* note 7, at 1836–43 (suggesting the development of an action for tortious enablement of criminal conduct or tortious conduct by website operators).

176. RESTATEMENT (SECOND) OF TORTS § 46(1) (1977); Citron, *Cyber Civil Rights*, *supra* note 5, at 88–89.

177. 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.”).

178. 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.

179. Citron, *Mainstreaming*, *supra* note 7, at 1818.

## C. CIVIL RIGHTS LAW

Professor Citron has recently suggested that a civil rights agenda might expand to combat certain cyber-abuses.<sup>180</sup> 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.<sup>181</sup> 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.<sup>182</sup> 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.<sup>183</sup> 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.<sup>184</sup> Additionally, many people's physical world employment opportunities may be affected negatively if employers have access to harmful information about an individual and decide not to hire or promote that individual. Additionally, employers may even terminate that individual's employment.

Civil rights suits entail some advantages, such as easing the costs of litigation for victims of online harassment<sup>185</sup> and reaching wrongs that would otherwise escape criminal or tort liability.<sup>186</sup> 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.

---

180. 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 . . .").

181. *Id.* at 91–92 (citing 42 U.S.C. § 1981 (2006) and 18 U.S.C. § 245(b)(2)(C) (2006), respectively).

182. *See* discussion *supra* Section I.A.3.

183. Citron, *Cyber Civil Rights*, *supra* note 5, at 92–93 (describing how 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").

184. MADDEN & SMITH, *supra* note 58, at 3 (noting that twelve percent of employed adults now report that they need to promote themselves online); Citron, *Cyber Civil Rights*, *supra* note 5, at 93 (describing how online attacks can be particularly intimidating for women and minorities, given that online attacks can often interfere with an individual's work).

185. Citron, *Cyber Civil Rights*, *supra* note 5, at 91 (noting that civil rights lawsuits have statutory damages that make pursuing such cases more affordable and attractive when compared to traditional tort suits).

186. *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.").

Enforcing authorities, including judges and, in some cases, the United States Attorney General,<sup>187</sup> 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 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 cyber-bullying. As noted above, cyber-bullies generally target individuals for reasons outside membership in a protected class.<sup>188</sup> Bullies may target people whom they perceive as a threat, or whom 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.

This survey of the limitations of criminal, tort, and civil rights laws evinces the fact that law in and of itself will never be a full solution to problems of cyber-victimization. While these laws serve an important expressive function and may apply to certain kinds of cyber-abuses, they need to be supplemented by extra-legal approaches to redressing online wrongs. Laws *per se* suffer from difficulties of identifying an anonymous or pseudonymous defendant and having effective jurisdictional reach over the defendant. This is particularly problematic in the case of disharmonized state criminal laws. Even if plaintiffs can identify their defendants—which may require an expensive and time-consuming court order—they are often judgment-proof. Attaching liability to online service providers for the comments of anonymous posters is also problematic because of the operation of § 230 of the Communications Decency Act. Many extra-legal approaches to cyber-abuse avoid these problems because they can protect a victim without requiring expensive and public litigation. Some of the more obvious of these approaches are discussed in the next Part.

#### IV. EXTRA-LEGAL APPROACHES TO ONLINE WRONGS

This Part examines several extra-legal regulatory approaches that could impact the ways in which people interact online. It focuses on regulatory

---

187. *Id.* at 93 (noting that the Attorney General can file civil suits for injunctive relief under Title VII of the Civil Rights Act of 1964).

188. *See* discussion *supra* Section I.A.2.

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, using abuse reporting hotlines, and creating 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.<sup>189</sup>

#### 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.<sup>190</sup> However, 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.<sup>191</sup> Relevant regulatory modalities will likely include social norms,<sup>192</sup> system architecture,<sup>193</sup> market forces,<sup>194</sup> public education,<sup>195</sup> and the use of private institutions.<sup>196</sup>

189. U.S. CONST. amend. 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.”).

190. Lawrence Lessig, *The Law of the Horse: What Cyberlaw Might Teach*, 113 HARV. L. REV. 501, 507–08 (1999) (suggesting four regulatory modalities for cyberspace: legal rules, social norms, market forces, and system architecture); Lawrence Lessig, *The Architecture of Privacy*, 1 VAND. J. ENT. L. & PRAC. 56, 62–63 (1999) (suggesting the same four norms of regulation for online privacy); Lipton, *supra* note 4, at 925 (“[L]egal regulation alone is unlikely to solve society’s video privacy problems.” Rather, “a multi modal approach that combines [the following] six regulatory modalities” may be necessary: “legal rules, social norms, system architecture, market forces, public education, and private non-profit institutions.”).

191. See, e.g., LAWRENCE LESSIG, CODE: VERSION 2.0, at 5 (2006), available at <http://codev2.cc/download+remix/Lessig-Codev2.pdf> (“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.”).

192. See Steven Hetcher, *Using Social Norms To Regulate Fan Fiction and Remix Culture*, 157 U. PA. L. REV. 1869 (2009) (discussing the role of norms in regulating online fan fiction and remix communities); Jacqueline D. Lipton, *Copyright’s Twilight Zone: Digital Copyright Lessons from the Vampire Blogosphere*, 70 MD. L. REV. 1 (2010) (discussing the development of norms of authorship and fan use of copyright works online); Jacqueline D. Lipton, *What Blogging Might Teach About Cybernorns*, 4 AKRON INTELL. PROP. J. 239 (2010) (discussing the development and identification of norms in the blogosphere); Mark Schultz, *Fear and Norms and Rock & Roll: What Jambands Can Teach Us About Persuading People To Obey Copyright Law*, 21

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,<sup>197</sup> technological solutions, and emerging social norms<sup>198</sup> that impact online behavior. Participants in online communities will also learn something from a legislature's willingness to proscribe certain conduct. Public education, through news stories, and publicly or privately funded education initiatives, is also an important part of the framework. Appropriately tailored educational initiatives will assist in the development of online norms.

## B. EMPOWERING VICTIMS TO COMBAT ONLINE ABUSES

### 1. Reputation Management Techniques

“Your online reputation is your reputation. Period.”<sup>199</sup>

A key to protecting individuals from online abuses is to empower those individuals to protect themselves without needing to resort to the legal system. This may be more complex than it sounds because protecting an individual's reputation involves both teaching an individual to be more careful about information she discloses about herself online and to attempt to monitor information that others disclose about her online. 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

---

BERKELEY TECH. L.J. 651 (2006) (discussing the role of norms in regulating copyrights in certain sectors of the music industry); 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.”).

193. LESSIG, *supra* note 191, at 5; Joel Reidenberg, *Lex Informatica: The Formulation of Information Policy Rules Through Technology*, 76 TEX. L. REV. 553 (1998) (describing how digital technology can be utilized as a regulatory mechanism for online conduct).

194. 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.”).

195. See Lipton, *supra* note 4, at 979–80.

196. *Id.* at 980–81.

197. For examples of private online reputation management services, see, e.g., REPUTATIONDEFENDER, <http://www.reputationdefender.com> (last visited May 20, 2010); YOUTHDILIGENCE, <http://www.youthdiligence.com> (last visited May 20, 2010).

198. See, e.g., OWN WHAT YOU THINK, <http://www.ownwhatyouthink.com> (last visited May 20, 2010) (campaign to promote more accountable and responsible online discourse).

199. FERTIK & THOMPSON, *supra* note 1, at 16.

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 to use maximum privacy protections on services such as Facebook<sup>200</sup> 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. This serves as a form of online insurance and potentially prevents negative content from making it onto the first page of search results about them.

It is also important to educate people about the risks inherent in releasing their personal information online. 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.<sup>201</sup> 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<sup>202</sup> and asking providers of online forums to monitor, police, and remove damaging content.<sup>203</sup> It may also involve knowing how to use other online tools, such as astroturfing, and search engine optimization to repair damage.<sup>204</sup>

---

200. 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, 10:55am), <http://blog.facebook.com/blog.php?post=391922327130>.

201. MADDEN & SMITH, *supra* note 58, at 2–3 (noting that individuals are indeed becoming more vigilant over time about self-monitoring and observation of information available about others online); Robert McGarvey, *Is Bad Taste the New Taste? Social Media Is Changing Our Sense of What's Acceptable—And What's Not*, THINK, Spring/Summer 2010, at 24, 26–27 (2010) (describing a situation in which 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).

202. FERTIK & THOMPSON, *supra* note 1, at 162–87.

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

204. *Id.* at 426–27 (describing the use of astroturfing by reputation management services such as ReputationDefender). Astroturfing involves seeding the Internet with positive or neutral content generated by the individual herself in an attempt to drown out the abusive content. The term “astroturfing” has arguably begun to take on negative connotations in the

Search engine optimization techniques involve the manipulation of search engine results so that positive or neutral information is prioritized in searches above harmful information.<sup>205</sup> Many of these tools are currently utilized by private online reputation management services. However, individuals can learn how to use them without having to pay the fees charged by the private services.<sup>206</sup> Some literature is now available to assist individuals in learning strategies that commercial reputation management services have typically utilized.<sup>207</sup>

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).<sup>208</sup> 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.<sup>209</sup> 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, third parties will have generated such materials.<sup>210</sup> Thus, the victim will not have a copyright claim that could support the use of the DMCA.<sup>211</sup>

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 engaging the services of a private reputation management company. While

---

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.

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

206. *See 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.").

207. 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 & THOMPSON, *supra* note 1.

208. 17 U.S.C. § 512(c) (2006).

209. § 512(c)(1)(C).

210. For example, a person who takes an embarrassing photograph of the victim will generally hold copyright in the photograph. *See* DANIEL J. SOLOVE, THE FUTURE OF REPUTATION: GOSSIP, RUMOR, AND PRIVACY ON THE INTERNET 184 (2007).

211. *See id.*

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<sup>212</sup> for doing a number of things that private individuals could do on their own if they knew how.<sup>213</sup> Cynically, one might also argue that private reputation management services actually benefit from online abuses and that it is in their own commercial interests for online abuses to continue to some extent.<sup>214</sup>

## 2. Education

The increased ability of private individuals to protect their 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,<sup>215</sup> such as libraries and universities. It may also be that private non-profit organizations, such as the Electronic Frontier Foundation<sup>216</sup> and the Electronic Privacy Information Center,<sup>217</sup> 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.

---

212. Bartow, *supra* note 14, at 423–26 (describing fees charged by ReputationDefender for its various services).

213. FERTIK & THOMPSON, *supra* note 1, at 235–47 (describing ways in which private individuals and small businesses can act to protect their own online reputations); Bartow, *supra* note 14, 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.”).

214. 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.

215. 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. Am. Library Ass'n Inc.*, 539 U.S. 194 (2003) (upholding legislation that required internet filtering as a condition of libraries accepting government funding).

216. See ELECTRONIC FRONTIER FOUNDATION (EFF), <http://www.eff.org> (last visited Apr. 20, 2010).

217. See ELECTRONIC PRIVACY INFORMATION CENTER (EPIC), <http://www.epic.org> (last visited Apr. 20, 2010).

A number of private organizations already provide information about online harms in addition to 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.<sup>218</sup> 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,<sup>219</sup> a government-sponsored educational initiative to protect children online.

Another service aimed at protecting children online is GetNetWise,<sup>220</sup> 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.<sup>221</sup>

### 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 their usefulness. 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,<sup>222</sup> typically for a monthly fee.<sup>223</sup> They then

---

218. See NETSMARTZ, <http://www.netsmartz.org> (last visited May 20, 2010).

219. See FVTC INTERNET CRIMES AGAINST CHILDREN TRAINING & TECHNICAL ASSISTANCE PROGRAM, <http://www.icctraining.org> (last visited May 20, 2010).

220. See GETNETWISE ABOUT... KIDS' SAFETY, <http://kids.getnetwise.org> (last visited May 20, 2010).

221. See *Tools for Families*, GETNETWISE ABOUT... KIDS' SAFETY, <http://kids.getnetwise.org/tools/toolscontracts> (last visited July 8, 2010).

222. 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, Xanga, Bebo, Flickr, LiveJournal, and many others for any material that might be damaging or distressing to a client . . .").

223. See *id.* ("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 and \$14.99 per month for its monitoring services. See YODILIGENCE, <http://www.youdiligence.com> (last visited June 5, 2011).

provide monthly reports to a client summarizing information about the client available online.<sup>224</sup>

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.<sup>225</sup> The client may even ask the service to target information that may be true.<sup>226</sup> 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.<sup>227</sup> Most reputation management services regard their techniques for sanitizing a person's online reputation as "proprietary"<sup>228</sup> and do not disclose those techniques publicly.<sup>229</sup> However, their methods likely include: (a) using notice and takedown procedures from the DMCA,<sup>230</sup> (b) contacting blogs and other web hosts and asking them to remove damaging information;<sup>231</sup> (c) astroturfing the Internet with newly manufactured neutral or positive information about their clients;<sup>232</sup> and (d) engaging in search engine optimization techniques to ensure that neutral and positive information about their clients is prioritized in search results.<sup>233</sup>

---

224. See Bartow, *supra* note 14, at 423 (citing ReputationDefender's "SEARCH" process).

225. See *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.").

226. *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"); *id.* at 425 ("ReputationDefender is also willing to mask or bury accounts of mainstream news stories even if they are true.").

227. FAQ, *Can You Help Remove Absolutely ANY Content from the Internet*, REPUTATIONDEFENDER, <http://www.reputationdefender.com/faq/> (last visited July 8, 2010) (describing the service's removal procedures and its limitations, such as its refusal to remove media articles, government records, and issues of "legitimate public interest").

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

229. *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 & THOMPSON, *supra* note 1.

230. 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 *supra* Section III.B.

231. 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.").

232. *Id.* at 426-27.

233. *Id.* at 427 ("Another avenue available to reputation defense organizations is Search Engine Optimizing, which has been characterized by at least one legal scholar as fraud. It is

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.<sup>234</sup> The use of private commercial services does not raise the specter of a First Amendment challenge. As noted above, many laws directed at curtailing online speech may raise First Amendment concerns and may be open to constitutional challenge.<sup>235</sup> 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.<sup>236</sup> Harmful content can simply be unobtrusively de-prioritized in search engine results.

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.<sup>237</sup> While engaging a service to monitor one's reputation on the Internet may be relatively affordable,<sup>238</sup> paying fees to repair one's online reputation may be prohibitive for many. Additionally, while these commercial services are available—at least to wealthier people—there may be less pressure on the government to act. If the government thinks the market is

---

an effort to manipulate search engine results for profit.”); Lidsky, *supra* note 8, at 1390 (describing services provided by commercial reputation management companies).

234. FERTIK & 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.”).

235. See, e.g., Diane Leenheer Zimmerman, *Is There a Right To Have Something To Say? One View of the Public Domain*, 73 *FORDHAM L. REV.* 297, 348–49 (2004).

236. Lidsky, *supra* note 8, at 1390 (“Hiring a reputation management company sometimes provides an attractive alternative to suing for libel because suing often brings more attention to the libelous statements.”).

237. Citron, *Cyber Civil Rights*, *supra* note 5, at 106 (“Few free or inexpensive resources are available for defending one's online reputation, and the services of groups like ReputationDefender are expensive and beyond the means of many victims.”).

238. The fees for monitoring one's reputation are typically in the ballpark of around \$10 to \$15 a month. See *supra* note 223; Bartow, *supra* note 14, at 424 (noting that ReputationDefender charges \$14.95 per month to monitor a client's online reputation).

handling the problem, government agencies may put less effort into investigating and prosecuting the abuses.<sup>239</sup>

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.<sup>240</sup> 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 service provider.<sup>241</sup> Recent statistics suggest that many online service providers will quickly remove harmful information on request.<sup>242</sup> 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' reputation may backfire dramatically. Most of them will not offer any guarantees of success<sup>243</sup> or refunds for backlash caused by their activities.<sup>244</sup> For example, one ReputationDefender client, Ronnie Segev, suffered a significant backlash as a result of ReputationDefender's efforts to remove embarrassing content

---

239. *Id.* at 422 (describing how market solutions benefit affluent parties that can afford services such as ReputationDefender but paradoxically decrease governmental incentive to provide low-cost solutions to individuals who are likely to need such services the most).

240. *See* discussion *supra* Section III.B.1.

241. *See* discussion *supra* Section IV.B.

242. MADDEN & SMITH, *supra* note 58, at 4 (noting that a significant majority of people who have sought removal of information about them posted online have been successful).

243. The disclaimer in YouDiligence's terms of service is a good example of how little these services guarantee in practice. *See Terms of Service*, YODILIGENCE, <http://www.youdiligence.com/yd/TermsOfUse.htm> (last visited May 20, 2010) (outlining the service's broad and strongly stated disclaimer of any warranties of any kind to customers).

244. 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 (noting how online attackers are likely to be emboldened when a victim attempts to stay online or fight back, as many attackers aim to force victims off the Internet).

about him from a website.<sup>245</sup> After ReputationDefender sent a notice to the website operator requesting removal of the harmful information,<sup>246</sup> a blogger from the website wrote a scathing post entitled “Ronnie Segev and ReputationDefender Can Eat a Dick.”<sup>247</sup>

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 sending harassing and abusive communications directly to a victim. In the Megan Meier scenario, for example, where harmful communications were 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 cyber-bullying and cyber-harassment laws if police and prosecutors are prepared to act on the complaints.<sup>248</sup>

#### 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,

---

245. Bartow, *supra* note 14, at 425–27 (discussing the Segev incident). The comments posted online were details of a scheme Segev was involved in during his youth to defraud Priceline of an airticket.

246. ReputationDefender sent the following 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.

*Id.* at 426.

247. *Id.*

248. See discussion *supra* Section II.A.

commercial services are expensive and out of the reach of many victims of online abuses.<sup>249</sup> At the same time, some of the tools they utilize are readily available to private individuals who know how to use them.<sup>250</sup> 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.

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 may not deal with many of these cases because they are unfamiliar with the relevant laws, or they may assess current law as inadequate to cover the victims' harms. 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.<sup>251</sup> 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

---

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

250. FERTIK & THOMPSON, *supra* note 1, at 234–47 (advising individuals and small businesses on techniques to self-protect online reputations).

251. Cohen-Almagor, *supra* note 3, at 426–27 (critiquing several existing Internet hotlines).

may be referred to a public authority.<sup>252</sup> 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.<sup>253</sup> Users can report such content in a variety of ways including submission of an online form.<sup>254</sup> In the United States, the CyberTipline is another example of a hotline for reporting certain damaging conduct much of which involves children, such as child prostitution, child molestation, and sex tourism involving children.<sup>255</sup>

Among the more salient advantages of hotlines in the context of online abuses is the fact that they can open up channels of communication between victims, observers of harmful conduct, and law enforcement authorities.<sup>256</sup> 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.<sup>257</sup> 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 by increasing awareness of damaging online conduct. This can enable individuals as well as 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.<sup>258</sup> 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

---

252. *Id.*

253. *See* INTERNET WATCH FOUNDATION (IWF), <http://www.iwf.org.uk/reporting.htm> (last visited May 19, 2010).

254. *Id.*

255. *See* NATIONAL CENTER FOR MISSING AND EXPLOITED CHILDREN, <http://www.missingkids.com> (last visited May 19, 2010).

256. Cohen-Almagor, *supra* note 3, at 427.

257. *Id.*

258. *See* NETANEL, *supra* note 158, at 104–05 (on law's expressive functions).

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,<sup>259</sup> a Princeton student created the Own What You Think website, asking students to pledge not to visit anonymous gossip sites and to be accountable for their own online communications.<sup>260</sup> The site sports the banner headline “Anonymity = Cowardice.”<sup>261</sup>

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.”<sup>262</sup> Even if we become desensitized to these kinds of communications, one would hope that we never become desensitized to dangerous and harmful conduct like cyber-bullying 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.

An example of the interplay between government and market self-regulation in the social networking context is the 2008 Joint Statement on Key Principles of Social Networking Sites Safety adopted between MySpace

---

259. Cohen-Almagor, *supra* note 3, at 419–20 (describing harmful online postings about college students on the juicycampus.com website).

260. See OWN WHAT YOU THINK, <http://www.ownwhatyouthink.com> (last visited May 19, 2010).

261. *Id.*

262. McGarvey, *supra* note 201, at 29.

and state Attorneys General.<sup>263</sup> These principles are aimed at protecting children from inappropriate and harmful online content.<sup>264</sup> They encompass strategies such as developing software tools to protect children from harmful content, designing social networking sites in a way that prevents minors from accessing inappropriate content, educating parents and children about online safety issues, and ensuring that social networking sites cooperate with law enforcement agencies in protecting children online.<sup>265</sup>

Companies might also be compelled to self-regulate if they were subjected to a system 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.<sup>266</sup> The hope is that by the government calling websites out on irresponsible behavior, websites would potentially regulate their own content.

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.<sup>267</sup> Google’s experimental Search Wiki enables Internet users to make comments on search results.<sup>268</sup> 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 way

---

263. MySpace and State Attorneys General, Joint Statement on Key Principles of Social Networking Sites Safety 1 (Jan. 14, 2010), <http://ago.mo.gov/newsreleases/2008/pdf/MySpace-JointStatement0108.pdf>.

264. *Id.*

265. *Id.*

266. Patrick Wintour, *Web Providers To Be Named and Shamed over Offensive Conduct*, THE GUARDIAN (Nov. 15, 2008), <http://www.guardian.co.uk/technology/2008/nov/15/internet-children>.

267. *See generally* FERTIK & THOMPSON, *supra* note 1, at 91 (describing these services).

268. *Id.*

to enable them. Additionally, anyone can comment on any search result, so there is no way for an Internet user to screen for true or false comments. Google now also offers a Google Profile service that enables individuals to write a brief profile about themselves.<sup>269</sup> These profiles may be displayed at the bottom of Google search results for personal names. 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. Additionally, they have limited use for people with common names.

The Wikipedia online dispute resolution service provides another form of self-regulation that could potentially protect one's online reputation. 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.<sup>270</sup> The participatory nature of Wikipedia means that an individual will not necessarily control information about her that may be posted on a Wikipedia page.<sup>271</sup> Wikipedia has its own online dispute resolution procedure to verify the accuracy of information posted, and individuals harmed by false or de-contextualized postings may utilize this service.<sup>272</sup> While this approach is specific to Wikipedia, other online service providers could adopt similar approaches if they want to assist their users in combating reputational harms.

## V. CONCLUSION

"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."<sup>273</sup>

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

---

269. *Id.*

270. *Id.* at 182 ("Wikipedia . . . is a free collaboratively edited encyclopedia. Anyone can edit any article, and anyone can create new articles.").

271. *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.").

272. *Id.* at 182–83 (describing applications of Wikipedia's dispute resolution procedure to reputational injuries).

273. Goodno, *supra* note 41, at 125.

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 they 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.<sup>274</sup> 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.

---

274. For example, governments are generally permitted to fund programs that impact speech. *See, e.g.*, *United States v. Am. Library Ass'n Inc.*, 539 U.S. 194, 194 (2003) (upholding a funding program that required libraries to filter internet access as a condition of accepting government funding).

