Washington University Law Review

Volume 87 | Issue 2

January 2009

Criminal Liability for Internet Culprits: The Need for Updated State Laws Covering the Full Spectrum of Cyber Victimization

Kate E. Schwartz
Washington University School of Law

CRIMINAL LIABILITY FOR INTERNET CULPRITS: THE NEED FOR UPDATED STATE LAWS COVERING THE FULL SPECTRUM OF CYBER VICTIMIZATION

I. INTRODUCTION

On October 16, 2006, Tina Meier found her thirteen-year-old daughter, Megan, hanging from a belt inside her closet.[1] The situation was a tragedy from the start for Tina and her husband, Ron, who pieced together what had seemingly pushed Megan to her unexpected suicide.[2] Megan had only gotten to know sixteen-year-old Josh Evans through the cloaked world of an internet social network after he contacted her on MySpace.[3] But when, after a month of flirtation, Josh inexplicably became cruel, Megan grew distraught.[4] The day before she took her own life, Josh had publicly posted her private messages, as well as his own harsh comments calling her "fat" and a "slut," for others to read and laugh at.[5] It was the very day that she died though, just twenty minutes before Megan went through with her act of suicide, that she had received a message from Josh telling her: "Everybody in O'Fallon knows how you are. You are a bad person and everybody hates you. Have a shitty rest of your life. The world would be a better place without you."[6]

It was not until six weeks later that the Meiers learned the true extent of the tragedy underlying their daughter's death; a young girl from the neighborhood came forward and informed them that Josh had never existed.[7] It turned out the fictitious boy had been created to "mess with

1. Christopher Maag, *A Hoax Turned Fatal Draws Anger but No Charges*, N.Y. TIMES, Nov. 28, 2007, http://www.nytimes.com/2007/11/28/us/28hoax.html?_r=1&oref=slogin.

2. *Id.* (explaining that, while Megan had spoken of suicide before, she had never acted upon such thoughts in the past, and she was not believed to be suicidal by her doctor or parents).

3. *Id*.

4. *Id*.

5. Andrew M. Grossman, *The MySpace Suicide: A Case Study in Overcriminalization*, 32 THE HERITAGE FOUND. 2 (2008), http://www.heritage.org/Research/ LegalIssues/lm32.cfm.

6. *See* Steve Pokin, *My Space Hoax Ends with Suicide of Dardenne Prairie Teen*, ST. LOUIS POST-DISPATCH, Nov. 11, 2007, http://suburbanjournals.stltoday.com/articles/2007/11/13/news/sj2tn 20071110-1111stc_pokin_1.ii1.txt (explaining that the FBI was not able to retrieve the final message from the Meier's computer hard drive, and that the quoted language is "according to Ron [Meier]'s best recollection," what he believes to be Josh's final message as he viewed it on Megan's MySpace account shortly after her death).

7. Maag, *supra* note 1; *see also* Pokin, *supra* note 6 (explaining that the girl who came forward to the Meiers had sent one message to Megan from the phony MySpace account, and that after the

Megan,"[8] not by a sixteen-year-old at all, but rather, by a forty-seven-year-old woman who lived four houses away from the Meiers in Dardenne Prairie, Missouri.[9] Lori Drew's original intent was apparently grounded in a desire to find out what Megan would say about her daughter, a former friend of Megan's.[10] There is no reason to believe that Drew actually intended to bring about Megan's death.[11] But, arguably, she deliberately participated in a ploy that would foreseeably cause an adolescent to suffer severe emotional distress.[12] The emotional distress that Megan endured as a result of the internet ploy was particularly foreseeable for Drew, because Megan had struggled with depression issues in the past[13] and Drew was aware of Megan's emotional fragility.[14]

---

ambulance arrived at the Meier's home, Drew had called the girl, instructing her not to disclose the MySpace hoax to anyone).

8. Maag, *supra* note 1.

9. *Id.*; *see also* Lauren Collins, *Friend Game*; *Behind the Online Hoax that Led to a Girl's Suicide*, THE NEW YORKER, Jan. 21, 2008, http://www.newyorker.com/reporting/2008/01/21/080121fa_fact_collins?currentPage=all ("Initially, a police officer wrote in a report that Lori Drew had 'instigated' and 'monitored' the account; she now contends the report is inaccurate, and has asserted that she merely agreed to the idea, which her daughter and Ashley Grills, the eighteen-year-old who worked for a direct-mail business that the Drews ran from their dining room, initiated."); Pokin, *supra* note 6 (explaining that, in addition to Drew and the neighbor that came forward, Drew's daughter and Drew's employee also allegedly contributed to the communication with Megan under the alias of "Josh" on the phony MySpace account).

10. Collins, *supra* note 9 ("The purpose of 'Josh Evans,' according to the Drews' testimony to Jack Banas [the prosecuting attorney for St. Charles County], was to ascertain whether Megan was making nasty remarks about their daughter, whom Megan had previously called a 'lesbian.'"); *see also* Pokin, *supra* note 6.

11. Pokin, *supra* note 6 (quoting Tina Meier: "'She wanted to get Megan to feel like she was liked by a boy and let everyone know this was a false MySpace and have everyone laugh at her. I don't feel their intentions were for her to kill herself. But that's how it ended'"); *see also* Pokin, *supra* note 6, (quoting Ron Meier: "'Ultimately, it was Megan's choice to do what she did,' he says. 'But it was like someone handed her a loaded gun.'").

12. *See* Collins, *supra* note 9. Whoever, exactly, came up with "Josh" conjured more than a perfunctory decoy. An online Frankenstein's monster, geared to the needs of an insecure, excitable teen-age girl, Josh's components were carefully chosen to exploit Megan's vulnerabilities. His profile picture was lifted from that of a handsome teen-age boy. He listened to Rascal Flatts, Korn, and Nickelback. His "turn-ons" included tongue piercings and being nibbled on the ear.

Playing on Megan's susceptibility to underdogs, Josh's creators endowed him with a pitiable bio: "when I was 7 my dad left me and my mom and my older brother and my newborn brother . . . poor mom yeah she had such a hard time . . . finding work to pay for us after he left." His ambitions also seemed tweaked to Megan's desires. His answer to the section "Goal you would like to achieve this year" was "meet a great girl." The girl he was looking for happened to have long brown hair, like Megan. As for weight, Josh answered, "DONT REALLY MATTER." *Id.*

13. *Id.* ("In the third grade, Megan told Tina that she wanted to kill herself. The Meiers took her to see a psychiatrist. Megan was prescribed Celexa (an antidepression drug), Concerta (for A.D.D.), and Geodon (a mood stabilizer).").

14. *See* Pokin, *supra* note 6 (explaining that, because the Drews had taken Megan with them on vacations, they were aware that she had a history of depression and that she took medication for her condition).

Since the hoax that preceded Megan's suicide became public knowledge, the incident has often been referred to as an unfortunate example of "cyberbullying."[15] However, scholarly discussions about "cyberbullies" tend to pertain to minors and the question of whether schools have the legal right to discipline them.[16] Lori Drew's behavior made it clear that cyberbullying is not limited to students targeting their peers, and that a solution extending beyond school discipline may be necessary.[17] While similar problems have been recognized amongst adults in the context of cyberharassment and cyberstalking, it is difficult to ascertain the difference between these three forms of internet victimization, especially because they are often used interchangeably. Ultimately, since there are no universal terms with corresponding sets of definitions to describe the acts that internet culprits commit,[18] scholarly discussions surrounding different forms of internet victimization have become muddled with confusing overlaps regarding both the ages of the persons involved and the severity of the culprit's conduct.[19] Such overlaps thwart clear analysis and the creation of successful solutions.

While many states have taken steps to account for the increased dangers posed by internet victimization, there is a need for more complete coverage in this area of law to account for the full spectrum of problematic behavior in the cyber context. This Note begins, in Part II, by presenting the current labels for victimizing internet behavior and their overlapping definitions as they are discussed in academic literature. Part III then explains why all forms of cyber victimization involve enhanced risks because of the internet's unique characteristics. Next, Part IV describes the current spectrum of state statutes in this area of criminal law, providing examples of how states' criminal codes do not account for all forms of cyber victimization independently. Part V then explains why states should

15. *See, e.g.*, Matthew C. Ruedy, Note, *Repercussions of a MySpace Teen Suicide: Should Anti-Cyberbullying Laws Be Created?*, 9 N.C. J. L. & TECH. 323, 326 (2008).

16. *See generally* Tracy L. Adamovich, Note, *Return to Sender: Off-Campus Student Speech Brought On-Campus by Another Student*, 82 ST. JOHN'S L. REV. 1087 (2008); Cara J. Ottenweller, Note, *Cyberbullying: The Interactive Playground Cries for a Clarification of the Communications Decency Act*, 41 VAL. U. L. REV. 1285 (2007); Renee L. Servance, Note, *Cyberbullying, Cyber-Harassment, and the Conflict Between Schools and the First Amendment*, 2003 WIS. L. REV. 1213 (2003).

17. Ruedy, *supra* note 15, at 328 ("The term 'bullying' brings up connotations of a schoolyard playground . . . [y]et as evidenced in Megan's case, 'cyberbullying' can occur anywhere and by anyone, regardless of age.").

18. Naomi Harlin Goodno, *Cyberstalking, a New Crime: Evaluating the Effectiveness of Current State and Federal Laws*, 72 MO. L. REV. 125, 147 (2007) ("While many states are taking active steps to combat the problem of cyberstalking, there is a complete lack of uniformity in defining the crime.").

19. *See* discussion *infra* Part II.

update their laws to impose criminal liability for all possible forms of cyber victimization. Finally, Part VI proposes a three-tiered classification of cyber victimization crimes that states could effectively implement. The scheme proposed in this Note accounts for conduct that is likely to pertain to minors, but it does not involve categorical distinctions based on age. Instead, the proposed scheme includes the possibility for both adults and young people to be held liable, but breaks down degrees of liability based on the culprit's intent and the victim's harm suffered.[20]

II. BLURRED CATEGORIZATIONS: THE TERMS USED TO REFERENCE FORMS OF CYBER VICTIMIZATION

The terms that scholars use to define various forms of cyber victimization lack clear distinctions, presenting an initial obstacle to creating effective solutions. Cyberstalking, cyberharassment, and cyberbullying are the most commonly used terms. The differences between these labels pertain to the ages of the parties involved and the severity of the victimizing acts at issue. As such, the terms largely blend together in scholarly commentary.[21]

First, the term cyberbullying is typically used in reference to juveniles or students, but it is unclear exactly which party must be a minor for the situation at issue to constitute cyberbullying. Some commentators consider cyberbullying to be the internet counterpart to traditional playground bullying, which presupposes that the culprit and the victim are both minors.[22] For others, the term is used to reference "the victimization of minors,"[23] regardless of whether the culprit is himself a minor or an adult.[24] A third definition for cyberbullying requires that the culprit be a

20. This test will balance the need for broader liability with concerns about over-criminalization by ensuring that the safety of individuals of all ages will be protected, but also that less egregious behavior does not have overly severe implications. *See* discussion *infra* Part VI.C.

21. *See* Sarah Jameson, Note, *Cyberharassment: Striking a Balance Between Free Speech and Privacy*, 17 COMMLAW CONSPECTUS 231, 236 (2008) ("One problem that often arises with the definition of cyberharassment is the interchangeable and synonymous use of the terms 'cyberharassment,' 'cyberstalking,' and 'cyberbullying.' Although the terms are similar, each is subtly distinct.").

22. *See, e.g.*, Ottenweller, *supra* note 16, at 1291 ("Cyberbullies are typically adolescent children, frequently in middle school, who direct hurtful and threatening comments at other adolescents over the Internet."); Servance, *supra* note 16, at 1218.

23. Ruedy, *supra* note 15, at 326.

24. *Id.* at 328 (defining cyberbullying as something which "can occur anywhere and *by anyone, regardless of age*") (emphasis added).

minor, but leaves open the possibility that the victim could be an adult, such as a teacher.[25]

The latter two uses of the term cyberbullying both contemplate the possibility that one party may not be a minor. These definitions overlap with what other commentators deem either cyberharassment or cyberstalking—terms that tend to be used in conjunction with adult behavior.[26] Furthermore, even though cyberstalking and cyberharassment typically pertain to adults, they may be used to reference situations involving cyber victimization in a school setting.[27] The overlap between these terms and cyberbullying can similarly be seen with respect to the degrees of harm inflicted by the culprit. According to the United States Department of Homeland Security's website for the United States Computer Emergency Readiness Team, schools are common problem areas, but cyberbullying "can affect any age group" and the actions at issue "can range in severity from cruel or embarrassing rumors to threats, harassment, or stalking."[28]

In addition to overlapping with cyberbullying, cyberharassment and cyberstalking can be largely indistinguishable from one another. For example, one commentator states that cyberstalking is distinct from cyberbullying because cyberstalking involves credible threats.[29] Another commentator states that cyberstalking includes the use of "electronic communication to stalk *or harass* another individual,"[30] suggesting that cyberstalking is not independent of cyberharassment[31] and need not involve credible threats.

One commentator uses the phrase "cyber targeting" because it "both reflects more accurately what is going on and indicates that it can include many potential legal causes of action." The advent of this unique phrase

25. *See* Todd D. Erb, Comment, *A Case For Strengthening School District Jurisdiction to Punish Off-Campus Incidents of Cyberbullying*, 40 ARIZ. ST. L.J. 257, 259 (2008) ("Cyberbullying is not just limited to students: teachers and administrators are also targeted by cyberbullies."); *see also* Jameson, *supra* note 21, at 237 ("cyberbullying often refers to cyberharassment *committed by* children) (emphasis added).

26. *See, e.g.*, Servance, *supra* note 16, at 1219 ("The term 'cyber-harassment,' as used in this Comment, denotes the targeting of adult members of the school community on the Internet.").

27. *See* Goodno, *supra* note 18, at 138 ("The cyberstalker was a fellow student . . . .").

28. Mindi McDowell, United States Computer Emergency Readiness Team, *National Cyber Alert System, Cyber Security Tip ST06-005, Dealing with Cyberbullies*, http://www.us-cert.gov/cas/tips/ST06-005.html (last visited Jan. 18, 2009).

29. Ruedy, *supra* note 15, at 326–27.

30. Goodno, *supra* note 18, at 126 (emphasis added).

31. *Id.* at 143. Here Goodno does note that some states have "harassment" laws and others have "stalking" laws; however, for the purpose of her article, she appears to encompass both of them in the internet context under only the single term cyberstalking.

highlights that using the more well-known terms for cyber victimization is difficult because the intended meanings of those terms may not be immediately apparent.[32] The discrepancies between the uses of these three terms in academic literature are similarly reflected in the inconsistencies amongst state laws dealing with cyber victimization.[33] However, before examining the range of state statutes, a discussion of the risks posed by cyber victimization is merited.

III. WHY ALL FORMS OF CYBER VICTIMIZATION INVOLVE ENHANCED RISK

The internet's unique characteristics enhance the risks associated with all forms of victimizing communications in two related ways: First, they make cyber victimization more prevalent than victimization in the physical world. Second, they amplify the dangerous effects of such communications upon the victim.[34] Stalking and harassing speech are already commonly understood as criminal acts in the non-internet world. Like harassing and stalking speech, however, bullying speech is also more damaging when it is communicated over the internet. [35] As such, speech intending a lesser degree of harm, such as humiliation, should not be overlooked in the internet context, even though these types of communications may implicate young adults. Indeed, even in the non-internet context "[b]ullying manifests a wide range of emotional harm, from low self-esteem, anxiety, and depression to social withdrawal."[36] A 2006 news article highlights the fact that these manifestations are a reality of cyberbullying as well, reporting that "[e]xperts and news reports worldwide tell disturbing tales of students harassed via the computer to the

32. David A. Myers, *Defamation and the Quiescent Anarchy of the Internet: A Case Study of Cyber Targeting*, 110 PENN ST. L. REV. 667, 668 (2006).

33. Jameson, *supra* note 21, at 237 ("Many state laws that address cyberharassment, cyberstalking, and cyberbullying combine the three types of cybercrimes in their statutory schemes.").

34. *See infra* notes 38–58 and accompanying text.

35. Ottenweller, *supra* note 16, at 1294 ("There are several reasons that cyberbullying on the Internet is arguably more damaging to children than typical schoolyard bullying."); *see also* Ruedy, *supra* note 15, at 328 ("Cyberbullying has the potential to have a far greater impact than traditional bullying because of the public nature of the Internet and the ease of distribution of information.").

36. Servance, *supra* note 16, at 1216; *see also* Berin Szoka & Adam Thierer, *Cyberbullying Legislation: Why Education is Preferable to Regulation*, PROGRESS ON POINT June 2009, at 4, *available at* http://www.pff.org/issues-pubs/pops/2009/pop16.12-cyberbullying-education-better-than-regulation.pdf (pointing to incidents of suicides by minors who were victims of anti-gay bullying in their schools, and noting that "[i]n a recent review of studies of bullying and suicide [by] researchers at the Yale School of Medicine . . . [a]lmost all of the studies found connections between being bullied and suicide.").

point that they've left school or become severely depressed. A teenager in New Zealand recently committed suicide after being inundated with dozens of harassing and insulting text messages."[37] The reasons for the enhanced risks associated with internet victimization apply, therefore, regardless of whether the parties involved are minors or adults.

To begin, one dangerous aspect of the internet is that it provides people with the ability to reach a vastly broader audience than ever before.[38] As a result, individuals are "no longer constrained by the volume of their voice"[39] when they send harmful messages over the internet, making it easier for the culprit to reach his victim, and likewise, more difficult for the victim to simply avoid his harasser.[40] The internet also allows these culprits to repeatedly victimize others with as little as the click of a button, requiring vastly less effort of stalkers, harassers, or bullies than in an off-line context.[41] Moreover, when damaging speech is posted on a website, the harm to the victim is public and constant, "which compounds the invasion of privacy and ultimately the impact . . . ."[42] The potential for humiliating online messages to be widely dispersed public knowledge is equally, if not more, daunting for young people, who tend to spend large quantities of their free time online as extensions of their social interactions.[43]

Another uniquely problematic feature of the internet is the fact that, when an occurrence sparks one's desire to communicate language meant to threaten, distress, or humiliate an individual, the internet diminishes any need for delay in carrying out that communication.[44] This in turn eliminates the likelihood that the individual will think about the effects of

37. Tim Grant, *Bullies Take Intimidation To Cyberspace*, PITTSBURGH POST-GAZETTE, June 26, 2006, http://www.post-gazette.com/pg/06177/701250-51.stm.

38. Scott Hammack, Note, *The Internet Loophole: Why Threatening Speech On-Line Requires a Modification of the Courts' Approach to True Threats and Incitement*, 36 COLUM. J.L. & SOC. PROBS. 65, 81–83 (2002). Hammack also distinguishes that, unlike the broad audience that people can send hurtful language to through other mediums, like television or books, "the on-line audience is . . . widely scattered, making it very difficult to identify and track down." *Id.* at 82.

39. *Id.* at 81.

40. Goodno, *supra* note 18, at 129 ("Cyberstalkers . . . can use the Internet to terrify their victims no matter where they are; thus, they simply cannot escape.").

41. *Id.* at 129 (comparing harassment over the phone, in which case "every telephone call is a single event that requires the stalker's action and time" with harassment via an "e-mail bomb," which only requires a harasser to draft a single e-mail, at which point the computer can be programmed to send it to the victim repeatedly).

42. *Id.*

43. *See* Collins, *supra* note 9 (explaining that for teenagers, social websites can serve as "a sort of popularity ledger" and describing that a teens' internet social life can be "more mercurial, and perhaps more crucial to their sense of status and acceptance, than the one they inhabited in the flesh").

44. Hammack, *supra* note 38, at 83.

his words and decide not to go through with the planned speech.[45] Instead, harmful language can be transmitted over the internet "in a fit of rage," and if the language is posted publicly in cyberspace it may be "impossible to delete and may continue to incite readers long after the speaker has moderated her position."[46] When harassing or bullying communications are at issue, the internet's instant nature may also encourage victims to lash out by acting in a harassing or bullying manner themselves, thus contributing to the cycle of victimization.[47]

Another aspect of the internet that increases the risk of cyber victimization is the ease with which a culprit may anonymously post harmful messages without repercussions. Since the internet provides speakers with "unprecedented anonymity," it "eliminates the social checks of ostracism and condemnation."[48] Additionally, anonymity makes it easier for the perpetrator to overcome personal inhibitions that might have deterred him from carrying out the victimizing behavior if he were confronting his victim face-to-face.[49] It is also less likely that the culprit will put an end to the harmful behavior because "reactions such as crying, which might lead people to realize that their comments have been carried too far or misinterpreted, are no longer visible."[50] Since the internet shields bullies from obtaining knowledge about the effects of their behavior, they can convince themselves that they are simply having fun when they annoy or humiliate their victims and, thus, justify continuing their behavior.[51] The internet's anonymity not only eases one's ability to victimize another individual, but also enhances the damaging effects on those who receive the victimizing messages. When speech communicated online involves more serious language, like threats, the anonymous delivery heightens the fear instilled in the victim, because "[w]hen a threat comes from an unknown source, the victim is unable to assess the threat accurately."[52]

---

45. *Id*. ("As a result, the immediacy of the speech makes it more likely that lawless action will ensue.").

46. *Id.*

47. *See* Ruedy, *supra* note 15, at 329 (explaining that, according to a recent study, seven percent of middle school students who had been cyberbullied "had served as both the bully and the victim on different occasions" (citing AMANDA LENHART ET AL., PEW INTERNET & AM. LIFE PROJECT, TEENS AND TECHNOLOGY: YOUTH ARE LEADING THE TRANSITION TO A FULLY WIRED MOBILE NATION (2005), http://www.pewInternet.org/pdfs/PIP_Teens_Tech _July2005web.pdf (on file with the North Carolina Journal of Law & Technology))).

48. Hammack, *supra* note 38, at 83.

49. Goodno, *supra* note 18, at 130.

50. Robin M. Kowalski & Susan Limber, *Electronic Bullying Among Middle School Students*, 41 J. ADOLESCENT HEALTH S22, S23 (2007).

51. Kowalski, *supra* note 50, at S28.

52. Hammack, *supra* note 38, at 84. In order to exemplify the effect that anonymity can have on

Likewise, the anonymity possible with cyberbullying can "leave a child wondering if each person he or she meets was potentially the perpetrator."[53] Regardless of age, the victim may be helpless to determine who or how many people are sending the message, leaving him uncertain of whether the message is meant to be taken seriously or whether any threats made are capable of being carried out.[54]

Finally, one of the most daunting aspects of internet victimization is the culprit's ability to take on the victim's identity.[55] By assuming the victim's identity, the culprit may cause third parties to become accomplices in the crime.[56] The incitement of third parties can be overt.[57] However, such incitement can also involve innocent third parties, which is often linked to the culprit's deceptive use of the victim's identity. For example, one individual harassed his victim by "impersonating her in various Internet chat rooms and posting her telephone number, address, and messages that she fantasized of being raped. Because of these messages, on separate occasions, at least six men knocked on the woman's door saying they wanted to rape her."[58] Without the internet's unprecedented anonymity and vast audience both at work, one can imagine how difficult it would be for a person to harass his victim by pretending to be her and inviting the involvement of unknowing third parties. Ultimately, the myriad of risks posed by the internet as a mode of stalking, harassing, and bullying

---

someone who is threatened, Hammack notes that if a disagreeable child threatens to shoot a neighbor with a BB gun, the neighbor can easily take appropriate actions such as calling the child's parents, avoiding him, or confronting him. However, if the same child sends the neighbor an anonymous email threatening to injure her, she has no means with which to counter the threat and no method for establishing its veracity. *Id.*

53. Kowalski, *supra* note 50, at S28.

54. Hammack, *supra* note 38, at 84.

55. Goodno, *supra* note 18, at 131. As an example of a cyberstalker taking on the identity of his victim, Goodno tells the story of Jane Hitchcock.

> [Mrs. Hitchcock] was cyberstalked by the owner of a company after she complained about the company's services. Intending to provoke others, the cyberstalker impersonated Hitchock and posted inflammatory comments on Web pages and sent e-mails in her name aimed at provoking others to "flame" her. . . . He would also send thousands of harassing messages to her husband's and her employer's e-mail accounts, sometimes impersonating Hitchcock, which eventually flooded the accounts rendering them 'useless.' The cyberstalker's actions became so unbearable that Hitchock was forced to physically move, but that did not stop him. He eventually found her online and would begin to harass her again. Hitchock sued him, but the cyberstalker was never held criminally liable.

Id. (citing J.A. HITCHCOCK, NET CRIMES AND MISDEMEANORS: OUTMANEUVERING THE SPAMMERS, SWINDLERS, AND STALKERS WHO ARE TARGETING YOU ONLINE 11 (Loraine Page ed., 2002)).

56. Goodno, supra note 18, at 132.

57. Hammack, *supra* note 38, at 82 ("Through email, discussion boards, and instant messaging, the Internet also facilitates the creation of networks of like-minded persons to help carry out threats.").

58. Goodno, *supra* note 18, at 132.

individuals necessitates careful consideration of how state laws account for internet-victimization crimes.

IV. THE SPECTRUM OF STATE LAWS

There has been nearly nationwide acknowledgement of the role that electronic communication can play in harming others. This acknowledgement is evidenced by the fact that most states have updated their laws to account for at least one form of cyber victimization.[59] However, a range of shortcomings still exist: First, three states still do not have laws which plainly address any form of cyber victimization. Additionally, many states account for the use of computers and the internet for one crime, but fall short of fully covering all potential forms of cyber victimization. Finally, a third category involves states with laws that conflate various types of harm into a single, overly inclusive statute.

A. States That Do Not Explicitly Criminalize Any Form of Cyber Victimization

As of this writing, there are only three states remaining with laws that do not plainly account for internet victimization of any kind: Nebraska,[60] New Jersey,[61] and New Mexico.[62] Each of these states has stalking and harassment laws which use broad definitions that include "communication" as a mode of carrying out the relevant crimes. However, these laws do not explicitly include the use of computers or electronic communications as a means of victimization.

Nebraska's stalking and harassment statute, for example, defines "course of conduct" for the purposes of these crimes 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."[63] This definition omits any reference to the internet. As such, the statute

59. *See* National Conference of State Legislatures, State Electronic Harassment or "Cyberstalking" Laws, http://www.ncsl.org/IssuesResearch/TelecommunicationsInformationTechnology/CyberstalkingLaws/tabid/13495/Default.aspx (last visited Aug. 3, 2009) (listing states that "explicitly include electronic forms of communication within stalking or harassment laws").

60. *See* NEB. REV. STAT. § 28-311.02 (2008) (stalking and harassment).

61. *See* N.J. STAT. ANN. § 2C:12-10 (West 2005) (stalking), § 2C:33-4 (harassment).

62. Harassment and Stalking Act, S.B. 166 (N.M. 2009) (enacted).

63. NEB. REV. STAT. § 28-311.02(2)(b) (2005).

leaves open the possibility for a culprit to, for example, post humiliating forms of communication on a website without potential criminal repercussions, since such posts may be construed as communications that are not directed at the individual.

Similarly, New Jersey's stalking and harassment statutes refer to "communications," but they do not directly reference the possibility that such communication will be transmitted over the internet.[64] There is, however, legislation pending in New Jersey which seeks to include broader forms of victimizing behavior that are made possible by the internet. Specifically, the legislation proposes to add the following language to the state's harassment law:

> A person commits a crime of the fourth degree if, in committing an offense under this section, he makes or causes to be made a communication or communications in violation of this section by electronic means, to persons other than the victim or in such manner that persons other than the victim may readily observe the communication or communications.[65]

This language would account for communications like website posts, which, as explained earlier in this section, are not easily encompassed by anti-victimization laws without reference to the internet. The legislation proposes to further amend the harassment statute by criminalizing communication "which exposes or publicizes any secret or any asserted fact, whether true or false, tending to subject another person to hatred, contempt or ridicule," and any course of conduct which is carried out with the purpose to "embarrass" or "humiliate" an individual.[66] If revised accordingly, New Jersey's harassment law would, therefore, more broadly account for bullying types of behaviors as well. This bill was introduced in the New Jersey Senate on March 9, 2009 and, as of this writing, has been referred to the Senate Judiciary Committee.[67]

New Mexico also currently has laws that define "pattern of conduct" without reference to electronic communications.[68] Like New Jersey, New Mexico had legislation pending that proposed to amend the harassment

64. *See supra* note 61.
65. S. 2704, 213th Leg., 2d Reg. Sess. (N.J. 2008).
66. *Id.*
67. New Jersey Legislature, http://www.njleg.state.nj.us/ (last visited Jan. 5, 2010) (input bill number in "Bill Search" section; then select "Search").
68. *See supra* note 62.

law to include such a reference.[69] However, as of this writing, action on that bill has been "postponed indefinitely."[70]

B. Problematic Aspects of Other States' Laws

While the vast majority of states have already worked to include cyber victimization in their criminal codes—either by creating new cyber statutes or by updating established stalking and harassment laws to cover acts carried out over the internet[71]—many of them have only addressed a single form of cyber victimization, and still others have seemingly criminalized multiple forms in one overly inclusive law.

Arizona is one such state that has addressed only a single form of cyber victimization. Under Arizona's harassment law, an individual who "[a]nonymously or otherwise contacts, communicates or causes a communication with another person by verbal, *electronic*, mechanical, telegraphic, telephonic or written means in a manner that harasses," commits a misdemeanor.[72] However, Arizona's stalking statute, which accounts for more severe behavior that causes a person to fear for his safety or life, does not directly include internet communications.[73] Therefore, if a culprit in Arizona stalks a person over the internet to the point of inflicting the requisite fear upon his victim, it may be difficult to convict the perpetrator of the felony crime.

Other states have grouped crimes involving various degrees of intent into a single, overly inclusive statute. Louisiana, for example, has a cyberstalking statute which criminalizes language communicated electronically "for the purpose of threatening, terrifying, *or harassing* any person."[74] This law imposes a fine of up to $2,000, up to 1 year in jail, or

---

69. S.B. 494, 49th Leg., 1st Sess. (N.M. 2009) (proposing to add the language "by any means, including an electronic communication device" to the harassment statue).

70. *See* New Mexico Legislature, SB 494 http://www.nmlegis.gov/lcs/_session. aspx?Chamber=S&LegType=B&LegNo=494&year=09 (stating that the bill's current location is "Died (API. [action postponed indefinitely])").

71. *See* Goodno, *supra* note 18, at 144–45.

72. ARIZ. REV. STAT. ANN. § 13-2921(A)(1) (2008) (emphasis added).

73. ARIZ. REV. STAT. ANN. § 13-2923 (2008).

74. LA. REV. STAT. ANN. § 14:40.3 (2007) (emphasis added). The statute's full definition explains:

> B. Cyberstalking is action of any person to accomplish any of the following:
>
> (1) Use in electronic mail or electronic communication of any words or language threatening to inflict bodily harm to any person or to such person's child, sibling, spouse, or dependent, or physical injury to the property of any person, or for the purpose of extorting money or other things of value from any person.

both for an initial offense, with increased fines and jail times possible for repeated offenses.[75] Kentucky serves as another example because, while it has a distinct law accounting for cyberstalking,[76] the state's harassing communications law appears to conflate cyberharassment and cyberbullying into a single law.[77] This statute first imposes criminal liability on an individual who, "with intent to intimidate, harass, annoy, or alarm another person," uses any form of written communication "in a manner which causes annoyance or alarm and serves no purpose of legitimate communication."[78] The statute then imposes the same degree of criminal liability on an individual who

> [c]ommunicates, while enrolled as a student in a local school district, with or about another school student, anonymously or otherwise, by telephone, the Internet, telegraph, mail, or any other form of electronic or written communication in a manner which a reasonable person under the circumstances should know would cause the other student to suffer fear of physical harm, intimidation, humiliation, or embarrassment and which serves no purpose of legitimate communication.[79]

Although many states have successfully taken affirmative steps to implement laws covering cyber victimization, others have fallen short. States that have amended their laws ineffectively, either by leaving them incomplete or making them overly inclusive, and states which have not amended their laws to include the internet at all should update their criminal codes to cover the full spectrum of cyber victimization.

---

(2) Electronically mail or electronically communicate to another repeatedly, whether or not conversation ensues, for the purpose of threatening, terrifying, or harassing any person.

(3) Electronically mail or electronically communicate to another and to knowingly make any false statement concerning death, injury, illness, disfigurement, indecent conduct, or criminal conduct of the person electronically mailed or of any member of the person's family or household with the intent to threaten, terrify, or harass.

(4) Knowingly permit an electronic communication device under the person's control to be used for the taking of an action in Paragraph (1), (2), or (3) of this Subsection.

Id.

75. *Id.*

76. H.B. 315 (Ky. 2009) (enacted) (amending stalking law to include the use of communication devices, such as computers and the internet, as a means by which the crime may be committed).

77. KY. REV. STAT. ANN. § 525.080 (West 2009).

78. *Id.* § 525.080(1).

79. *Id.* § 525.080(1)(c).

V. WHY STATE LAWS SHOULD BE UPDATED TO ACCOUNT FOR ALL FORMS OF CYBER VICTIMIZATION

While the law has since been amended,[80] Missouri's outdated harassment law prior to Megan Meier's death simply did not account for the circumstances of Drew's actions. Since Missouri legislators had not originally accounted for the unique modes of victimization made possible by the internet when they drafted the state's relevant criminal statutes, law enforcement authorities were powerless take any action against Drew or the other individuals responsible for harassing Megan Meier on the internet.[81] The aftermath of the Megan Meier incident demonstrates various reasons why states that have not done so already should impose criminal liability for acts of cyber victimization, and why states that have taken initial steps to expand their laws in this area should continue to do so in order to ensure complete coverage of cyber victimization.

This part first explores the pervasive and heightened effects of internet victimization that pose a problem of growing signficance. Next, this part explains the risk of over-criminalization resulting from attempts to hold internet victimizers legally responsible when no law on point exists. Finally, this part addresses the lack of other legal safeguards to serve as alternate remedies for individuals who are victimized online. Thus, when

---

80. MO. REV. STAT. § 565.090 (2009), *amended by* S.B. 818, 94th Gen. Assemb., 2d Reg. Sess. (Mo. 2008). The amended version of Missouri's harassment statute reads:

> 1. A person commits the crime of harassment if he or she:
>
> (1) Knowingly communicates a threat to commit any felony to another person and in so doing, frightens, intimidates, or causes emotional distress to such other person; or
>
> (2) When communicating with another person, knowingly uses coarse language offensive to one of average sensibility and thereby puts such person in reasonable apprehension of offensive physical contact or harm; or
>
> (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
>
> (5) Knowingly makes repeated unwanted communication to another 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.

Id.

81. Maag, *supra* note 1. According to Lieutenant Craig McGuire of the St. Charles County Sheriff's Department, Drew's conduct "might've been rude, it might've been immature, but it wasn't illegal." *Id*. The original statute specified how the harassing communication must be carried out, with no specific reference to the possibility of electronic communication. *See supra* note 80.

viewed as a whole, the factors explored in this part explain why states should update their laws to account for all potential forms of internet victimization.

A. Evidence of the Serious and Widely Felt Effects of Internet Victimization

Statistical evidence demonstrates that a significant portion of young people and adults alike have suffered from internet victimization at some point in their lives. The National Crime Prevention Council released information in 2007 stating that, in that year, forty-three percent of teenagers had been targeted by cyberbullies.[82] In fact, according to some commentators, "academic research suggests that peer-on-peer cyberbullying is a more significant online safety concern than child predation—and that this problem is growing," as evidenced by various teen suicides that have resulted from acts of cyberbullying.[83] Similarly, a 1999 Department of Justice report suggested that that the number of yearly cyberstalking incidents might be in the "tens of thousands."[84] The fact that these statistics reflect a grave potential for harm to the victims involved is evident by the correlating responses of legislators,[85] website creators,[86] and the general public.[87]

First, recent bills calling for education and prevention of internet victimization indicate that both national and state legislatures are in fact recognizing the realities about the prevalence of this problem in the modern age.[88] For example, on May 14, 2008, the Internet Crime Prevention Act was introduced in the United States Senate proposing that the Attorney General shall be directed to provide "grants for Internet crime prevention education programs."[89] Similarly, on May 22, 2008, the

82. National Crime Prevention Council, *Stop Cyberbullying Before it Starts*, http://www.ncpc.org/topics/by-audience/parents/bullying/cyberbullying/cyberbullying.pdf (last visited Jan. 6, 2010).

83. Szoka, *supra* note 36, at 4.

84. Goodno, *supra* note 18, at 126.

85. *See infra* notes 88–93 and accompanying text.

86. *See infra* notes 94–99 and accompanying text.

87. *See infra* notes 100–04 and accompanying text.

88. Szoka, *supra* note 36, at 2 ("In the 110th session of Congress, for example, more than 30 measures were introduced aimed at addressing child safety concerns in one way or another, although only a few of them passed into law.").

89. Internet Crime Prevention Act of 2008, S. 3016, 110th Cong. § 2 (2008). Section 2(c)(2) states that "[t]he term 'Internet crime prevention education program' means a program that serves to educate parents, children, educators, and communities about how to recognize and prevent potentially criminal activity on the Internet." *Id.* Section 2(c)(3) states that "[t]he term 'potentially criminally activity' includes access through the Internet and other electronic devices to potentially illegal activity

Protecting Our Children Online Act was introduced in the United States House of Representatives, proposing that the Communications Act of 1934 be amended to ensure that certain schools and libraries begin "educating minors about safe online behavior."[90] An Illinois statute exemplifies that states are also going to greater lengths to account for the increasing need for protection online.[91] Beginning in the 2009–2010 school year, Illinois law effectively mandates that an internet safety component be incorporated for children in or above third grade.[92] This modified version is distinct from the former law's mere suggestion that schools incorporate such a component into their curriculum.[93]

Legislative recognition of the serious nature of modern internet victimization problems mirrors the response of website creators and the general public. The "MySpace" website's home page,[94] for example, offers users a page dedicated to providing information on safety,[95] which is broken down into categories such as safety tips "for parents and educators"[96] and safety tips "for teens."[97] Aside from safety information being incorporated into pre-existing social networking sites, the creation of various new websites for the purpose of calling attention to these issues is indicative of the public's growing awareness and concern. Such websites cover a broad spectrum. For example, two individuals with PhDs in criminal justice created the website cyberbullying.us to serve as "a central repository and information clearinghouse for the phenomenon of cyberbullying."[98] Another website, cyberstalked.org, was created by a

---

including sexual or racial harassment, cyberbullying, sexual exploitation, exposure to pornography, and privacy violations." *Id.*

90. Protecting Our Children Online Act, H.R. 6145, 110th Cong. (2008). Sections 2(a)(3)(b), (i) and (ii) state that education about internet behavior "may include information about—interacting with other individuals through social networking websites, chat rooms, electronic mail, bulletin boards, instant messaging, and other means of online communication; and cyberbullying awareness and response." *Id.*

91. 105 ILL. COMP. STAT. ANN. 5/27-13.3 (West Supp. 2009).

92. *Id*.

93. *Id.* Section (c) replaced the former text, "[i]t is hereby recommended that the curriculum provide for a minimum of 2 hours of Internet safety education each school year," with language that orders, "a school district must incorporate into the school curriculum a component on Internet safety to be taught at least once each school year to students in grade 3 or above." *See* S.B. 2512, 95th Gen. Assem., Reg. Sess. (Ill. 2008).

94. MySpace Home Page, http://www.myspace.com (last visited Jan. 6, 2010).

95. *Id.* (follow "Safety" hyperlink).

96. *Id.* (follow "for parents & educators" hyperlink).

97. *Id.* (follow "for teens" hyperlink). This page also has a specific section dedicated to cyberbullying, with instructions on what to do if you are being victimized, and resources for teens who do not feel comfortable going to an adult for help. *Id.* (follow "Cyberbullying" hyperlink).

98. Cyberbullying Research Center, http://www.cyberbullying.us/aboutus.php (last visited Jan. 18, 2009).

former victim of cyberstalking to expose the injustices done by the internet culprit who preyed upon her, and to educate others.[99]

Finally, the public outcry regarding the lack of criminal liability originally imposed against Drew after the Megan Meier incident indicates the need for appropriate criminal laws punishing internet abuses against others.[100] In one of her articles, Kim Zetter points out the tendency for the cycle of internet victimization to be perpetuated when the legal system fails to impose criminal liability for abusive acts online.[101] Specifically, Zetter discusses Sarah Wells who, upon learning about the aftermath of the Meier incident, "resolved to take matters into her own hands."[102] Wells' actions demonstrate that people have an instinctive desire to punish internet culprits with a taste of their own medicine when the law is helpless to impose justice.[103] According to Zetter, after Wells tracked down Lori Drew's identity and posted the woman's name on her personal blog,

> her readers and other bloggers followed by finding and posting her husband's name, the family's address and phone number, a cellphone number, the name of the family's advertising company, and the names and phone numbers of clients with whom they worked . . .
>
> . . . .
>
> In retaliation, readers called Drew's advertising clients to urge them to withdraw their business from her. But it wasn't long before

99. http://www.cyberstalked.org/ourstory/ (last visited Jan. 18, 2009) [hereinafter Cyberstalked Website]; *see also* www.cyberangels.org (follow "About Us" hyperlink) (last visited Jan. 18, 2009) ("In response to citizens' calls for assistance in dealing with online threats, the Guardian Angels launched CyberAngels in 1995. Today CyberAngels is one of the oldest and most respected online safety education programs in the world."); www.bullypolice. org (last visited Jan. 18, 2009) ("A Watch-dog Organization—Advocating for Bullied Children & Reporting on State Anti Bullying Laws").

100. Collins, *supra* note 9 (stating that "public opinion against the Drews had been harsh, verging on violent," and describing that "Pam Fogarty, the mayor [of Dardenne Prairie], had two hundred unanswered e-mails in her in-box. 'People are shocked, and they're pissed as hell!'").

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

102. *Id.*

103. *Id.* ("The impulse is human nature, say experts, and few can imagine an offense more egregious than a trusted adult preying on the emotions of a vulnerable child. Shunning wrongdoers, especially in the absence of legal redress, helps maintain order and preserve a community's moral sense of right . . . .").

> there were death threats, a brick through a window and calls to set the Drews' house on fire.[104]

Thus, statistics regarding the prevalence of internet victimization are bolstered by the actions that legislators, website creators, and members of the general public have taken in recognition of the serious nature of this growing problem.

B. The Risk of Over-Criminalization When No Law On Point Exists

In addition to catching the public's attention, the lack of legal avenues available in Missouri to prosecute Drew for her behavior toward Megan Meier caught the attention of federal prosecutors.[105] Drew was indicted in Los Angeles, where MySpace is based, in February of 2008.[106] The indictment included one charge of conspiracy and three other charges relating to violations of the Computer Fraud and Abuse Act,[107] which was originally intended to criminalize hacking.[108] Specifically, "[t]he indictment allege[d] that Drew and her co-conspirators violated MySpace's terms of service, which require registrants to provide truthful registration information and refrain from soliciting personal information from anyone under 18 or using information obtained from MySpace services to harass or harm other people, among other terms."[109] In November of 2008, a jury found Drew guilty of "three misdemeanor offenses of accessing computers without authorization."[110] Recently, however, Drew was acquitted of those charges based on "the absence of minimal guidelines to govern law enforcement," and "actual notice deficiencies" in the applicable statute.[111]

---

104. *Id.*

105. See Kim Zetter, *Lori Drew Indicted in MySpace Suicide Case—Updated*, WIRED, May 15, 2008, http://blog. wired.com/27bstroke6/2008/05/lori-drew-indic.html [hereinafter Zetter, Indicted].

106. Grossman, *supra* note 5, at 3–4.

107. 18 U.S.C. § 1030 (2000).

108. Grossman, *supra* note 5, at 4. Criminal hacking is defined as "the surreptitious breaking 'into the computer, network, servers, or database of another person or organization.'" *See* Charlotte Decker, *Cyber Crime 2.0: An Argument To Update The United States Criminal Code To Reflect The Changing Nature Of Cyber Crime*, 81 S. CAL. L. REV. 959, 965 (2008) (quoting BLACK'S LAW DICTIONARY 730 (8th ed. 2004)).

109. Zetter, *Indictment, supra* note 105.

110. *See Conviction on Lesser Charges in MySpace Case*, MSNBC, Nov. 26, 2008, http://www.msnbc.msn.com/id/27928608?GT1=43001 (last visited Oct. 18, 2009) [hereinafter *Lesser Charges*] ("The federal jury could not reach a verdict on the main charge against 49-year-old Lori Drew—conspiracy—and rejected three other felony counts of accessing computers without authorization to inflict emotional harm.").

111. United States v. Drew, No. CR 08-0582-GW, 2009 WL 2872855, at *14 (C.D. Cal. Aug. 28, 2009).

Andrew Grossman, of the Heritage Foundation, joined with other groups[112] in criticizing the charges brought against Drew, claiming they were a classic example of over-criminalization.[113] Grossman opined that, "[w]hatever Drew intended to do, hacking MySpace was not it."[114] He expressed concern that social networks' terms of service are too vague to be the basis of criminal liability when violated, and that under the prosecution's theory of Drew's criminal liability, countless numbers of well-intentioned individuals could be subject to prosecution.[115] The United States District Court for the Central District of California echoed these concerns in its decision.[116] As an example of someone who could face criminal prosecution under the prosecution's application of the statute, the court pointed to "the lonely-heart who submits intentionally inaccurate data about his or her age, height and/or physical appearance, which contravenes the [MySpace.com Terms of Use Agreement] prohibition against providing 'information that you know is false or misleading.'"[117] While the court determined that "basing a CFAA misdemeanor violation . . . upon the conscious violation of a website's terms of service runs afoul of the void-for-vagueness doctrine," it appeared to leave open the possibility that such a conviction could be upheld if the statute's currently deficient notice and guidelines for law enforcement were appropriately revised.[118]

Despite the fact that Drew was not successfully prosecuted under the Computer Fraud and Abuse Act, her attempted prosecution under a statute that was arguably distantly related to her behavior demonstrates the need for states to enact statutes which will appropriately cover each type of

112. *See, e.g.*, Robert McMillan, *Group Says MySpace Cyber-bully Prosecution Goes Too Far*, PC WORLD, May 19, 2008, http://www.pcworld.com/businesscenter/article/146069/group_says_myspace_cyberbully_prosecution_goes_too_far.html ("[T]he Center for Democracy & Technology warned that the U.S. Department of Justice's action against Lori Drew . . . [went] too far by using an anti-hacking law to prosecute the O'Fallon, Missouri, woman for violating MySpace's terms of service.").

113. *See generally* Grossman, *supra* note 5. According to Grossman, over-criminalization defines the result that occurs when a "vague law" is "twisted" to encompass some particular conduct that already took place, in turn "expand[ing] [the law's] scope enormously." *Id.* at 1.

114. *Id.* at 6; *see also* McMillan, *supra* note 112 (quoting Brock Meeks, a spokesman for the Center for Democracy & Technology, as saying: "Everybody that is sympathetic to this case and saying finally we've got something to nail her on here, they're not looking hard enough at the fact that the Justice Department blundered by using this anti-hacker law.").

115. Grossman, *supra* note 5, at 7–8.

116. *See Drew,* 2009 WL 2872855.

117. *Id.* at *16.

118. *Id.* at *14; *see also id.* at *16 (noting, for example, that the statute's relevant provision "is not limited to instances where the website owner contacts law enforcement to complain about an individual's unauthorized access or exceeding permitted access on the site").

victimization possible in the internet context. In failing to address cyber victimization altogether, or in accounting for only some forms of the behavior, states leave open two possibilities: individuals will either successfully target their victims online without risking criminal liability, or they may face the potential to be charged with violating laws that do not truly pertain to their actions and intent.[119] Neither outcome is desirable, and both serve as reasons that states should update their laws accordingly.

C. The Lack of Other Legal Safeguards

In addition to the serious effects of cyber victimization and the potential for these acts to be over-criminalized when no appropriate law exists, the lack of other legal safeguards provides an additional reason for states to impose criminal liability where it is currently lacking. First, while civil sanctions may present one option for victims of internet harassment to gain relief, civil remedies are not, standing alone, sufficient or appropriate to deal with internet victimization issues. One problem is that "[t]he primary civil remedy available for cruel and insulting speech is a defamation action, or one of its subsets—libel or slander."[120] Internet harassment in one of its various forms has the potential to have serious negative effects on the victim, and yet not qualify under any of those causes of action.[121] For example, in *J.S. v. Bethlehem Area School District*,[122] a website created by one student and comments made on it by a number of other students, were so severely distressing to the targeted teacher that the teacher became mentally and physically ill and ultimately left the job.[123] Despite these consequences for the teacher, however, "the jury did not find the comments defamatory in nature."[124] Additionally, as one commentator explains, when students are the victims hoping to bring civil actions,

---

119. *See* Derek Kravitz, *'MySpace Suicide' Case Expands Web Law*, WASH. POST, Nov. 28, 2008, http://voices.washingtonpost.com/washingtonpostinvestigations/2008/11/myspace_suicide_ruling_a_water.html?nav=rss_blog ("Phil Malone, director of the Cyberlaw Clinic at Harvard Law School, said that [the verdict against Drew] could have a chilling impact given that the 'vast majority of Internet users do not read Web site terms of service carefully or at all.'").

120. *See* Erb, *supra* note 25, at 276–77 (2008) (citation omitted).

121. *See generally id.* at 276–80.

122. 807 A.2d 847 (Pa. 2002).

123. Erb, *supra* note 25, at 278 (explaining that the website made about the teacher listed reasons why she should be fired, depicted her as Hitler, and called for students to lend money for the cause of helping to "hire a hitman to kill her") (citing 807 A.2d 847 (Pa. 2002)).

124. Erb, *supra* note 25, at 278 (citation omitted).

> an entirely new set of problems arises. In a libel action, for example, the accused can use the affirmative defense that the hurtful statements are true. In cases where the comments are sexually explicit, such as listing which girl on campus is the "biggest "ho"' [sic] or which one performs the best oral sex, the civil nature of the case leaves open the unsavory possibility of a defense team setting out to prove that the student really was the "biggest ho" in the school.[125]

Furthermore, even if there is an applicable cause of action, the simple well-known fact that "[c]ivil lawsuits are expensive"[126] will often prevent injured parties from bringing suit based on limited resources. As part of her story about being targeted by an internet stalker, Cynthia Armistead states: "Legal advisors have since told me that there was more than enough evidence to obtain a civil judgment, but I did not have the resources to pursue a civil case . . . when the case was 'fresh'."[127] Armistead's perspective, as someone who has directly faced internet abuse, highlights the fact that costs and difficulties of maneuvering and understanding the legal system present hurdles that would impede many victims from pursuing civil redress. Without applicable criminal laws, therefore, such injured persons will probably never see their victimizer held accountable for his actions in a court of law. Additionally, while a civil action would potentially provide a victim with financial compensation, that victim's foremost priority will be ensuring that the culprit's behavior is put to an end. Accordingly, cyber victimization is better suited to prosecution under criminal law, which seeks to punish and deter wrongdoing, than liability under civil law, which seeks to make a person whole.[128]

Section 230 of the Communications Decency Act serves as another impediment to judicial relief, because it effectively prevents Internet Service Providers (ISPs) from being held civilly liable for the content that they passively publish over the internet.[129] Accordingly, websites themselves rarely provide any type of safeguard to protect individuals

---

125. *Id.* at 279 (citation omitted).

126. *Id.*

127. Cyberstalked Website, *supra* note 99.

128. *See, e.g.*, Wendy Gerwick Couture, *White Collar Crime's Gray Area: The Anomaly of Criminalizing Conduct Not Civilly Actionable*, 72 ALB. L. REV. 1, 44 (2009) ("[S]cholars typically agree that the criminal law punishes and deters and that the civil law compensates.") (citation omitted).

129. 47 U.S.C.A. § 230 (2000).

targeted on the internet.[130] In fact, "[m]ost courts interpret the CDA as giving ISPs complete immunity from legal action for the postings of a third party even if the ISP is notified about the harassing material and fails to take action."[131] The unfortunate result of this Communications Decency Act provision is, oftentimes, that no one is held responsible for the content that causes victims of internet abuse to suffer serious consequences.[132] If no criminal liability exists for the individual internet harasser, this result is especially likely to be true.

Finally, in the young adult context, it is important to recognize that schools are not fully capable of dealing with students who perpetrate internet abuse. In her article, Renee Servance notes some people's belief "that there is a strict line between on-and off-campus speech that removes school authority, with the underlying policy that schools have no right to usurp the role of parents."[133] Students that victimize others online, outside of school, are arguably beyond schools' authority. Contrary to the limited authority that schools hold, criminal liability gives courts the right to go beyond parents and impose punishments when such is a necessary means of carrying out justice. Furthermore, while in-school education about cyberbullying would certainly aid in prevention, "there is simply no substitute for parental oversight and mentoring," something which often goes overlooked by parents who are "[u]naccustomed to, or uncomfortable with modern computing or communication devices."[134] If state statutes were to hold minors responsible for paying fines in the event that they intentionally cause harm to another individual over the internet, parents would be forced to take notice of their children's behavior and, most likely, would quickly become involved in monitoring and advising their children's online activities.

---

130. *See* Erb, *supra* note 25, at 279 ("[P]arents have had little success using the Communications Decency Act in convincing Internet service providers to shut down cyberbullying web sites.") (citation omitted).

131. Ottenweller, *supra* note 16, at 1287.

132. Myers, *supra* note 32, at 671 ("This controversial provision has resulted in rather broad immunity for ISPs, and may, in some cases, leave no one legally accountable for the injuries caused by anonymous postings on the Internet.").

133. Servance, *supra* note 16, at 1222.

134. Szoka, *supra* note 36, at 19.

VI. HOW STATE LAWS SHOULD BE UPDATED: PROPOSAL OF A THREE-TIERED CLASSIFICATION FOR CYBER VICTIMIZATION CRIMES

Since each of the various degrees of cyber victimization has grown increasingly pervasive, states should adopt a three-pronged classification of such crimes. This scheme would include cyberstalking, cyberharassment, and cyberbullying in order to account for the various degrees of intent with which culprits may act—harshly punishing those that are malicious, and imposing lesser penalties on those that are less grave—to drive home the point that victimizing behavior will not be tolerated in our society. The lack of clear distinctions between these three labels as they are currently used, however, mandates that new standards be established to distinguish between each crime.

A. Consistent Elements Among All Three Cyber Crimes

1. The Culprit's Actus Reus

First, the culprit's method of victimization, or rather, his actus reus, should have no bearing on which crime is attributed to him. Perpetrators can communicate threatening, harassing, or offensive language to their victims using various methods.[135] All of the available methods that effectively victimize another individual over the internet should pertain to each of the types of cyber crimes alike.

Next, the definitions of all cyber crimes should be drafted so they dispel with the problematic actus reus requirements, which currently render many non-cyber stalking and harassment statutes inapplicable in the internet context.[136] Specifically, none of the crimes should require an element of proximity to the victim,[137] nor should they include an "overt" or "credible" threat requirement.[138]

---

135. These methods of interference can include e-mails or instant messages sent directly to the victim, offensive blog entries or comments posted about the person, or the creation of entire web pages negatively targeting the individual. *See* Ottenweller, *supra* note 16, at 1290.

136. *See* Goodno, *supra* note 18, at 134–39.

137. A proximity requirement would make it too problematic to impose liability on individuals who victimize their targets online because the fact that the crimes are carried out over the internet allows the perpetrator "to be hundreds or thousands of miles away from his victim." *Id.* at 135.

138. There are multiple reasons that no "overt" or "credible" threat requirement should be included. *Id.* at 135–39.

First, culprits can instill very real fear in their victims without explicitly threatening them. *Id.* at 136. Goodno points to *Iowa v. Limbrecht*, 600 N.W. 2d 316 (Iowa 1999), which was decided after Iowa updated its stalking law to use a reasonable-person standard in place of the formerly used

Finally, for all three crimes, the applicable actus reus should include a requirement of repetitive conduct. It is important that repetition be incorporated for all of the crimes because "punishing merely one instance of harassing conduct may unjustly penalize one who acts once out of anger, verses one who engages in a series of terrifying acts."[139] Even though each of the crimes should involve some degree of repetitive conduct, the extent or duration of the repetition required need not be the same for all three offenses, since it may serve as an indication of the perpetrator's intent (see discussion *infra* Part B).[140] The number of times the communicated act must be repeated, or the length of time that public language must remain posted on a website to inflict distress before qualifying as criminal, should be left to the trier of fact's discretion, so long as the perpetrator is not convicted for a single or fleeting act.

---

credible-threat standard, to demonstrate that stalking need not involve a threat. Goodno, *supra* note 18, at 136.

> The *Limbrecht* defendant, a prison inmate, became obsessed with a young woman, Stacey Corey, who worked as an employee at the prison. The defendant's repetitive, intimidating stares and lies to other inmates about how he had sexual relations with her forced Corey to quit and move. However, the defendant's obsession continued when he was released from prison. He found Corey's new address and sent vulgar, untrue letters to Corey's husband about how Corey had sexual relations with many inmates when she worked at the prison. The defendant also drove by Corey's house a number of times, which ultimately led to his arrest and stalking conviction. . . . Under the amended version of the statute, which adopted the reasonable person standard, the court found that the defendant's actions assumed frightening proportions and was no less threatening than an actual threat.

Id. at 136–37 (citing 600 N.W.2d at 316–19).

Second, "[a] 'threat' suggests a communication directly from the stalker to the victim," but there are various methods by which perpetrators can interfere with their victims indirectly online, such as creating a website that targets them. Goodno, *supra* note 18, at 138. A third problem is that this requirement places an "onerous and unnecessary" burden on the victim to show that the perpetrator was capable of carrying out the threat, while "the victim may not even know the true identity or location" of the person victimizing him. *Id.*

Finally, "[i]n situations where, for example, the cyberstalkers take on the identity of the victim and post messages inviting gang rape, there is neither an overt threat, nor a threat sent from the cyberstalker directly to the victim." *Id.* at 139. As this example demonstrates, each of the crimes must account for communications by the culprit that intentionally cause the victim to suffer from unwanted contact by innocent third parties.

139. *Id.* at 134. Furthermore, since physical proximity and credible threat requirements, which may have warranted criminalizing conduct without repetition, are dispensed of in this scheme, there is an enhanced need to require repeated conduct before imposing criminal liability.

140. When the method of victimization used only requires a single act by the culprit, but still produced ongoing distress for the victim, such as the creation of a website or a public blog entry, the duration that the site is left visible to the public and the number of "hits" from the public can serve as the indicators of "repetition."

2. The Age of the Parties Involved

Since it is increasingly evident that young people and adults alike are using the internet to victimize individuals, the age of the offender should not be a primary distinguishing factor in and of itself. Young people are capable of acting with malicious intent. On the other hand, adults can cause harm to another with bad, but less malicious, intent. While one's age is not dispositive of the degree of his intent, age may play a role in the context of the *relationship* between the perpetrator and the victim. In turn, the parties' relationship triggers different degrees of intent attributed to the culprit and thus different degrees of punishment.[141] As one commentator exemplified,

> [i]f an adult male called an adult female a "slut," the comment would not likely support a cause of action in civil court; likewise, the same comment posted on a web site about a thirteen year-old girl would not support a cause of action, *even though the young girl could be dramatically more affected than her adult counterpart*.[142]

The criminal scheme should account for the discrepancy in intentional acts that would clearly harm a minor, even though the same act might not harm an adult.[143]

3. A Clause Eliminating Constitutionally Protected Speech from the Statute's Reach

In order to ensure that speech constitutionally protected by the First Amendment is not implicated, all three criminal laws should contain two provisions: First, the laws should provide that the speech at issue "does not serve a legitimate purpose." Second, the laws should include a statement

---

141. For example, when something objectively hurtful, but not necessarily malicious, is communicated, a reasonable person would expect a child's reaction to be more severe than an adult's. A reasonable person would also expect an adult to be more conscious than a child of the fact that such an action serves no legitimate purpose. Thus, inherently, adult perpetrators of harmful communication online are held to a higher standard than minors, and minors inherently require a lesser threshold when they are targeted as victims.

142. Erb, *supra* note 25, at 279 (emphasis added).

143. This will be especially evident when an adult is targeting a minor, but should be analyzed on a case-by-case basis regarding the facts specific to the circumstances of the culprit and victim involved. Acts by minors should not necessarily be entirely left out of the criminal scheme though. As cyber crime expert Jayne Hitchcock said of cyberbullying: "'Honestly, it's harassment and stalking . . . for kids and teens, we call it bullying. But it's basically the same thing.'" Tim Grant, *Orie: Make Cyber Bullying A Crime In State*, PITTSBURGH POST-GAZETTE, June 27, 2006, http://www.post-gazette.com/pg/06178/701401-51.stm.

that the statute does not include constitutionally protected speech or activities.[144] With these provisions in place, criminal laws covering all three forms of cyber victimization can be upheld, because it is well established that "the right to free speech is not absolute."[145]

B. Distinguishing Elements Between the Three Cyber Crimes

1. The Perpetrator's Specific Intent and the Victim's Reasonable Reaction

This proposed scheme involves a combined subjective test, for the perpetrator's intent, or mens rea, and objective test, for the victim's reaction. A combined test is ideal because, while each one standing alone has shortcomings,[146] each one also provides an important protection to ensure that criminal liability is not improperly imposed. "The inclusion of a subjective intent standard prevents punishment of innocuous speech misunderstood by a recipient . . . ."[147] Therefore, the perpetrator's actual intent with regard to his victimizing acts should always be "willful," even though the severity of the culprit's willful intention will differ for each crime. That said, "an objective test is far more predictable and results in less self-censorship than its subjective counterpart."[148] Accordingly, all cyber crimes should assess the victim's harm suffered using a reasonable person standard, even though the degree of objectively reasonable harm suffered will differ for each crime.

The three cyber crimes are broken down under this proposed scheme by the following hierarchical system: First, cyber*bullying* is the least egregious of the crimes in terms of both the perpetrator's intent and the

144. *See* Commonwealth v. Welch, 825 N.E.2d 1005, 1018–19 (Mass. 2005) (listing decisions in which states "have construed their statutes that proscribe harassing conduct or speech as constitutionally permissible," most commonly because they "contain some combination of the following limiting characteristics: a 'willful,' 'malicious,' or specific intent element; a requirement that the conduct be 'directed at' an individual; a reasonable person standard; a statutory limitation that the conduct have 'no legitimate purpose'; and a savings clause excluding from the statute's reach constitutionally protected activity or communication.").

145. State v. Compas, 964 P.2d 703, 706 (Mont. 1998). "Indeed, there are certain well-defined and narrowly limited classes of speech, the prevention and punishment of which have never been thought to raise any Constitutional problems. One of those classes of speech not protected by the First Amendment is activity intended to embarrass, annoy or harass." *Id.* (internal citations and quotations omitted).

146. Hammack, *supra* note 38, at 96–100.

147. *Id.* at 97–98.

148. *Id.* at 101.

harm accordingly suffered.[149] Cyber*harassment* requires a stronger degree of intent and harm.[150] Finally, cyber*stalking* constitutes the most serious offense.[151] Since an objectively reasonable standard is used to assess the victim's reaction, criminal liability would not ordinarily be imposed where a victim only suffers because he is particularly vulnerable. However, if a perpetrator has personal knowledge of his victim's unique susceptibility before targeting the victim, such knowledge should be considered in conjunction with the culprit's degree of culpability.[152]

2. The Criminal Penalty Imposed on the Culprit

In light of the varying degrees of ill-will attributed to perpetrators of each cyber crime, and the varying degrees of harm suffered by victims of each cyber crime, different penalties should be imposed to appropriately reflect these distinctions.[153] States could, for example, make cyberbullying a simple violation or petty offense, punishable by a fine, with increased fines or degrees of culpability for repeat offenses. Cyberharassment could be a misdemeanor, imposing a higher fine or up to a year jail time for a first offense, and the potential for an increase to a stalking charge for a repeat offense. Cyberstalking, the most serious of the crimes, could be a felony subjecting those held guilty to the highest fines and the potential to serve greater jail time.

C. Why This Proposed Scheme is Ideal and How It Would Look in Effect

This scheme is ideal because it would ensure that juveniles and adults alike are held accountable for cyber victimization, but it would only

149. Cyberbullying should be found to occur when a person intentionally and repeatedly engages in behavior over the internet that serves no legitimate purpose, which the person should reasonably expect to cause the targeted individual to feel annoyed, humiliated, or ridiculed, and which would cause a reasonable person emotional distress.

150. Cyberharassment should be found to occur when a person intentionally and repeatedly engages in behavior over the internet that serves no legitimate purpose, which the person should reasonably expect to cause the targeted individual to feel harassed, alarmed, or intimidated and which would cause a reasonable person emotional distress.

151. Cyberstalking should be found to occur when a person maliciously and repeatedly engages in behavior over the internet that serves no legitimate purpose, which the person should reasonably expect to cause the targeted individual to feel terrorized, tormented, or fearful for his or her safety and which would cause a reasonable person to suffer ongoing fear or emotional distress.

152. The culprit's awareness of the targeted individual's vulnerability, if likely to enhance his resulting emotional distress, is indicative of a stronger degree of ill-intent.

153. While specific penalties will inevitably vary by state, the important distinction in this scheme is that penalties be distinguishable and adequately reflect the distinct degree of criminal liability attributed to each crime.

impose penalties appropriate to the severity of the crime in each possible situation.

First, in the peer-to-peer context, minors could be held liable for victimizing fellow minors online. Take, for example, a particular past situation involving seniors in high school "that posted the sexual history, names, and addresses of their fellow female students on a website [and] were initially charged with second-degree harassment, which carries a sentence of up to one year in jail and a $1,000 fine."[154] In that case, the charges were soon after dropped because the "District Attorney announced that, although the material on the web site was 'offensive and abhorrent,' it did not meet the legal definition of harassment."[155] Under the scheme proposed in this Note, the students could have been liable for cyberbullying if they acted with the requisite intent, because a jury would likely find that a reasonable woman would feel humiliated if such information was posted on the internet without her permission or initial knowledge. Likewise, a jury would probably find that the perpetrators should have reasonably expected the victimized women to suffer emotional distress when they learned what was posted about them.[156]

The possibility of minors using the internet to victimize adults, such as teachers or school administrators, presents another scenario. In light of the current unclear distinctions for acts of cyber victimization, this presents a gray area that is currently difficult to categorize. In the *J.S. v. Bethlehem Area School District* case previously discussed,[157] this scheme would impose criminal liability where civil and criminal remedies failed before.[158] In this case, the websites created by students stating why their teacher should be fired and depicting their teacher as Hitler were not technically defamatory, but as "the presiding judge stated . . . '[t]hey were a lot of other things: They were distasteful, they were rude, they were

154. Erb, *supra* note 25, at 275 (internal citation omitted).

155. *Id.*

156. Furthermore, this scheme makes it more likely that young people will truly be held liable for victimizing their peers. Currently, as Erb explained, "[i]n the rare cases where a student is criminally convicted of Internet harassment, appellate courts have been reluctant to enforce such penalties." *Id.* Since, under this proposed scheme, a cyberbullying offense would not impose the harsh punishment of jail time, appellate courts would likely be less reluctant to enforce the penalty. The imposition of a significant fine would still be effective, however, because it would likely prevent students from repeating such behavior in the future. It may also make parents more aware of and interested in monitoring their children's behavior on the internet. *See Lesser Charges*, *supra* note 110 (recognizing, according to U.S. Attorney Thomas, the "worthy message" that was sent by the jury's decision to convict Lori Drew: "'If you have children who are on the Internet and you are not watching what they are doing, you better be.'").

157. *See supra* text accompanying notes 123–24.

158. Erb, *supra* note 25, at 277–78.

crude, they were obscene.'"[159] Under the proposed scheme, the students' actions would at least qualify as cyberbullying since they could reasonably have expected that the offensive websites would upset and humiliate their teacher, whose resulting emotional distress manifested itself both mentally and physically, ultimately driving the educator to stop teaching.[160]

Next, as the Megan Meier incident demonstrates, there can also be problems with adults victimizing minors online.[161] This, too, currently falls into a gray area that is difficult to categorize. For example, literature surrounding the Megan Meier incident typically refers to cyberbullying[162] because the victim was a minor and the perpetrator acted under the guise of a minor. However, the fact that Drew was actually an adult makes that categorization seem out of place. Under the proposed scheme, the fact that Drew was an adult preying upon a minor, of whose vulnerable mental state she was aware,[163] makes her intent more malicious, and would likely raise this to the level of cyberharassment.

Finally, when adults victimize adults online, the proposed scheme could, as with the other scenarios, potentially impose liability under any of the three crimes depending on the specific circumstances of the case. Regardless of the crime attributed to the culprit in a particular adult-to-adult scenario, the proposed scheme would account for the unique circumstances of the internet where many current state statutes on regular harassment or stalking fail to suffice.

VII. CONCLUSION

The internet has advanced modern communication by providing people with innumerable benefits. Yet, those same advancements have also enhanced the ease and frequency with which people harboring animosity toward others can victimize targeted individuals. The prevalent use of the internet by adults and minors alike has rendered internet victimization an expansive problem reaching people of various ages and circumstances. In light of this modern trend, states should impose criminal liability

159. *Id.* at 278.

160. *Id.*

161. *See infra* text accompanying notes 1–14.

162. Kravitz, *supra* note 119 ("In what legal experts are calling the country's first cyber-bullying verdict, a Missouri mother has been convicted of impersonating a teenage boy online in a hoax that led to a young girl's suicide.").

163. ABC News, *Parents Want Jail Time for MySpace Hoax Mom*, Nov. 29, 2007, http://abcnews.go.com/GMA/Story?id=3929774&page=1 ("Megan sometimes suffered from low self-esteem and was on medication at the time of her death. 'That is what makes it even more disgusting, that she knew the circumstances around our daughter and still played on it,' said Megan's father, Ron Meier.").

following a scheme that accounts for perpetrators and victims of any age, and that distinguishes degrees of punishment based on the severity of the situation. Such laws would correctly punish those who intentionally act in a foreseeably harmful way toward others over the internet, deterring the continuance of such conduct by perpetrators and bringing justice to the victims who suffered as a result.

Kate E. Schwartz[*]

---

* J.D. Candidate (2010), Washington University School of Law; B.A. English (2007), University of Michigan. I would like to thank my parents for their constant guidance and support, and express my sincere gratitude to the *Washington University Law Review* editors for the hard work they contributed to the publication of this Note.