CYBERHARASSMENT: STRIKING A BALANCE BETWEEN FREE SPEECH AND PRIVACY

By Sarah Jameson[†]

I. INTRODUCTION

In October 2006, Missouri teenager Megan Meier committed suicide.[1] A year later, the thirteen-year-old's parents reported that Megan hanged herself due to a prank played by their forty-seven-year-old neighbor, Lori Drew, on MySpace.com.[2] The small town tragedy was dubbed the "MySpace Suicide Hoax."[3] Drew created a MySpace profile for a fictional boy named Josh Evans with the intention of discovering whether Megan spread rumors about her daughter.[4] Over the course of two hours on the night of Megan's suicide—in an incident prompted by the fake profile—Megan was the target of intense harassment.[5] Described as "a teenage mob on the Web," the attack spread rumors that Megan was fat, a slut, and that no one should befriend her.[6] Later that night, Megan's parents found her body hanging in her bedroom closet.[7] The local and national television news and talk radio shows broadcast the story, and bloggers wrote about it.[8] Tamara Jones, staff writer for the *Washington Post*,

---

† J.D. and Communications Law Studies Certificate Candidate, May 2009, The Catholic University of America, Columbus School of Law. A special thanks to Steve Klitzman and Karen Duquette for their guidance and assistance in the development of this Comment.

1 Lauren Collins, *Friend Game: Behind the MySpace Suicide*, NEW YORKER, Jan. 21, 2008, at 34.

2 *Id.*

3 *Id.*

4 TheSmokingGun.com, Megan Meier Police Reports: Cops Chronicle MySpace Hoax that Ended in 13-Year-Old's Suicide, http://www.thesmokinggun.com/archive/years/2007/1120072megan1.html (last visited Sept. 8, 2008) (providing background information and the actual police reports).

5 *See* Tamara Jones, *A Deadly Web of Deceit*, WASH. POST, Jan. 10, 2008, at C1.

6 *Id.*

7 TheSmokingGun.com, *supra* note 4 (providing the St. Charles County Sheriff's Department report for the incident).

8 *See* Jones, *supra* note 5 ("The troubling story was picked up by bloggers, talk radio

described the effect of Megan's death on the Internet community: "Tens of thousands joined the ongoing debate. Some wanted legislation; others wanted blood. On message boards and Web site memorials, in chats and forums, Megan would be mourned, analyzed, romanticized, vilified and endlessly discussed, giving her death the popularity she never knew in life."[9]

Over the next few months, the FBI investigated the Drew family's involvement in the incident.[10] The U.S. Attorney's Office and the St. Charles County, Missouri prosecutor initially decided that charges could not be filed against Lori Drew, her family, or their family friend, Ashley Grills, who participated in the prank.[11] The prosecutors determined that "no statutes against harassment, stalking or child endangerment could be applied here. What happened to Megan was despicable . . . but for it to be considered criminal the state would have to prove that the hoax was intended to frighten or disturb Megan, not merely elicit information."[12]

However, on May 15, 2008, Lori Drew was indicted for her role in the MySpace suicide hoax on one count of conspiracy and three counts of computer fraud under the Computer Fraud and Abuse Act.[13] This was the first time that a federal statute that applies to accessing protected computers was used for a social-networking case.[14] Although the government previously has filed charges against computer hackers under the Computer Fraud and Abuse Act, the statute has never been used to prosecute a cyberharasser.[15] In July 2008, representatives for Drew challenged the prosecution's use of the statute and filed a motion to dismiss.[16] Consistent with what some legal experts argue, the prosecution's use of the statute undermines the intent of the law—to punish and deter hackers from breaking into computer systems to steal private information.[17] While a great effort is being made to bring to justice those whose harassment led to Megan Meier's death, without a specific statute in place that penalizes cyberharassment, punishing those responsible likely will prove unsuccessful.

Megan's story is just one illustration of the potentially drastic consequences

---

and other in the indignant chat universe.").

9 Jones, *supra* note 5.

10 *Id.*

11 *Id.* Drew sometimes dictated to Ashley Grills the messages from the fictional boy. *Id.*

12 *Id.*

13 18 U.S.C. § 1030 (2000).

14 Linda Deutsch, *Teen's Neighbor Charged in Death*, WASH. POST, May 16, 2008, at C3.

15 *See id.*

16 Peter Whoriskey, *Woman Accused in MySpace Suicide Case Seeks to Have All Charges Dismissed*, WASH. POST, July 24, 2008 at D1.

17 *See* Editorial, *Falsehoods on MySpace*, WASH. POST, May 26, 2008, at A16; *see also* Whoriskey, *supra* note 16.

of cyberharassment. Commonly classified as a misdemeanor in most states, traditional harassment statutes have no applicable law or punishment for violators in cyberspace.[18] However, many states, including Missouri, either have enacted criminal laws against cyberharassment or established task forces to create such laws.[19] The Federal Government is recognizing slowly the growing problem,[20] but Congress has not yet enacted a criminal law punishing cyberharassment. Still, legislators realize that existing federal laws that address traditional forms of harassment either are too broad or too narrow and essentially ineffective.[21] If the law is too broad, it threatens to chill forms of speech and potentially violate the First Amendment.[22] If too narrow, a statute will not provide relief for a victim of cyberharassment because Internet Service Providers ("ISPs"), under section 230 of the Communications Decency Act ("CDA"),[23]

---

[18] *See* Harry A. Valetk, *Cyberstalking: Navigating a Maze of Laws*, 228 N.Y.L.J., July 23, 2002 at 5.

[19] *Id.* ("At last count, 41 states . . . had laws expressly prohibiting harassing conduct through the Internet, e-mail, or other electronic means."). On June 30, 2008, the Governor of Missouri, Matt Blunt, signed a bill that outlawed cyberharassment. Press Release, Missouri Governor Matt Blunt, Gov. Blunt Enacts Legislation to Safeguard Missourians from Internet Harassment (June 30, 2008), *available at* http://governor.mo.gov/press_June2008.htm (follow hyperlink of title). The measure broadened Missouri harassment law to include, in addition to harassment that is written or communicated over the phone, harassment over computers, text messages, and various electronic devices. *See* Associated Press, *Mo. Governor Signs Anti-Cyberbullying Bill into Law*, FIRST AMENDMENT CENTER, July 1, 2008, http://www.firstamendmentcenter.org/news.aspx?id=20245.

[20] On May 22, 2008, U.S. Representatives Kenny Hulshof (R-Mo.) and Linda Sanchez (D-Ca.) introduced H.R. 6123, The Megan Meier Cyberbullying Prevention Act, which would amend Title 18 of the U.S. Code to include federal penalties for cyberharassment. *See* Megan Meier Cyberbullying Prevention Act, H.R. 6123, 110th Cong. sec. 3 (2008); *see also Mo. Governor Signs Anti-Cyberbullying Bill into Law*, *supra* note 19. The legislation states

> § 881. Cyberbullying
>
> (a) Whoever transmits in interstate or foreign commerce any 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, shall be fined under this title or imprisoned not more than two years, or both.
>
> (b) As used in this section—
>
> (1) the term 'communication' means the electronic transmission, between or among points specified by the user, of information of the user's choosing, without change in the form or content of the information as sent and received; and
>
> (2) the term 'electronic means' means any equipment dependent on electrical power to access an information service, including email, instant messaging, blogs, websites, telephones, and text messages.
>
> (b) Clerical Amendment- The table of sections at the beginning of chapter 41 of title 18, United States Code, is amended by adding at the end the following new item:
>
> "881. Cyberbullying."

Id.

[21] *See infra* Part IV.

[22] U.S. CONST. amend. I ("Congress shall make no law . . . abridging the freedom of speech, or of the press . . . ."). *See infra* Part IV.B.

[23] 47 U.S.C. § 230 (2000).

cannot be held liable for the actions of third parties on their servers.[24]

In an increasingly digital world, as a person's privacy and reputation become more vulnerable to corruption, and anonymity via the Internet becomes more feasible, cyberharassment likely will increase and a federal law to curb or punish it will be necessary. However, the First Amendment right to free speech and the relative lack of government regulation of the Internet[25] stand as substantial obstacles to overcome to protect the privacy and reputation of individuals online.

This Comment discusses how cyberharassment, illustrated by the suicide of Megan Meier, is a serious threat to public safety. To mitigate the threat, this Comment proposes legislation criminalizing cyberharassment. Part II of this Comment defines cyberharassment and describes characteristics of the Internet that serve as cyberharassment facilitators. Part III discusses recent examples of cyberharassment, both intentional and unintentional, and the concerns these incidents raise about the protection of personal privacy and reputation. Part IV analyzes and critiques current federal law and commentary related to cyberharassment and the impact of existing laws on cyberharassment. Part V discusses and analyzes existing state laws and other policies that address cyberharassment and proposes sample legislation that would make cyberharassment a crime without violating the First Amendment. Enactment of a federal statute will ensure consistent prosecution of cyberharassers and proper relief for their victims while encouraging greater public safety on the Internet.

II. CYBERHARASSMENT: AN EXISTING PROBLEM AGGRAVATED BY NEW TECHNOLOGY[26]

A. Definition

Since Megan Meier's suicide, harassment over electronic mediums is the

---

[24] For an in depth discussion of the Communications Decency Act, see *infra* Part IV.

[25] Some regulations, primarily in the area of child protection laws, affect the Internet. *See* Children Online Privacy Protection Act, 15 U.S.C. §§ 6501–06 (2006). Generally, however, the United States has adopted a hands-off approach to Internet regulation. *See* Kevin A. Meehan, *The Continuing Conundrum of International Internet Jurisdiction*, 31 B.C. INT'L & COMP. L. REV. 345, 354 (2008) (explaining that a model of Internet regulation—the neo-mercantilism model—where the role of government "is to ensure the free flow of commerce along the information superhighway and to remove any impediments" is known as the "American approach to Internet regulation").

[26] Language taken from U.S. DEP'T OF JUSTICE, OFFICE OF JUSTICE PROGRAMS, 1999 REPORT ON CYBERSTALKING: A NEW CHALLENGE FOR LAW ENFORCEMENT AND INDUSTRY (1999), http://www.usdoj.gov/criminal/cybercrime/cyberstalking.htm [hereinafter 1999 DOJ REPORT].

subject of increased debate.[27] Harassment in its traditional offline form is defined as "words, conduct, or action . . . that . . . annoys, alarms, or causes substantial emotional stress in [the] person and serves no legitimate purpose."[28] Computers add another dimension to this definition and increase opportunities for online persecutors to harass their victims.[29] The ease with which a person can use e-mail or create a blog,[30] for example, facilitates the ability of harassers to assail their victims either in the home or in the workplace.[31] Additionally, if the harasser so chooses, he can remain anonymous, creating an even greater sense of unease for his victim.[32]

Although cyberharassment has no universal definition,[33] it typically occurs when an individual or group with no legitimate purpose uses a form of electronic communication as a means to cause great emotional distress to a person.[34] In addition to e-mail and blogs, conduits of "new media"[35] available to the cyberharasser include chat rooms, instant messaging services, electronic bulletin boards,[36] and social networking sites.[37] The Internet provides cyberhar-

---

27 *See* Chris Blank, *Mo. Teen's Suicide Inspires Bill*, FOXNEWS.COM, Jan. 29, 2008, http://www.foxnews.com/wires/2008Jan29/0,4670,InternetSuicide,00.html.

28 BLACK'S LAW DICTIONARY 733 (8th ed. 2004).

29 Paul Cullen, *Computer Crime*, *in* LAW AND THE INTERNET: REGULATING CYBERSPACE 207, 217 (Lilian Edwards & Charlotte Waelde eds., 1997) ("[C]omputers can provide a powerful tool for the criminally minded.").

30 *See* DANIEL J. SOLOVE, THE FUTURE OF REPUTATION: GOSSIP, RUMOR, AND PRIVACY ON THE INTERNET 20 (2007). The author commented

> All you need to do is go to one of the popular blogging websites, and you can set up an account for free (or at most, a few bucks per month). Some popular blogging websites include Blogger or Typepad. To set up your blog, you merely need to choose a name for it and a template for its look and style. In less that three minutes, you'll become a blogger, and with the click of a mouse, you can broadcast your thoughts live to the entire planet.

Id.

31 *See* Cullen, *supra* note 29, at 217.

32 *Id.*

33 *See* Valetk, *supra* note 18; 1999 DOJ REPORT, *supra* note 26.

34 *See In re* Standard Jury Instructions in Criminal Cases, 953 So. 2d 495, 496 (Fla. 2007).

35 Eileen M. Alexy et al., *Perceptions of Cyberstalking Among College Students*, 5 BRIEF TREATMENT AND CRISIS INTERVENTION J. 279, 279 (2005) (referring to the "the emergence of communication technologies" as "new media").

36 A bulletin board system, synonymous with a message board, is "an electronic message system running on a microcomputer. Call up, leave messages, read messages. The system is like a physical bulletin board . . . . Some people call bulletin board systems electronic mail systems." HARRY NEWTON, NEWTON'S TELECOM DICTIONARY 179 (22d ed. 2006).

37 David Harvey, *Cyberstalking and Internet Harassment: What the Law Can Do*, DAVID HARVEY, AUSTRALIAN INSTITUTE OF CRIMINOLOGY, NETSAFE.ORG.NZ 2 (2003), http://www.netsafe.org.nz/Doc_Library/netsafepapers_davidharvey_cyberstalking.pdf. Popular social networking sites include MySpace, Facebook, and Friendster. MySpace.com, About Us, http://www.myspace.com (follow "About" hyperlink) (last visited Oct. 25, 2008); Facebook.com, About Facebook, http//www.facebook.com/facebook (last visited Oct. 25, 2008);

assers with an easy channel to "incite others against their victims."[38] Not only can the cyberharasser harass his victim, but he can also impersonate the victim and post defamatory messages on bulletin boards, cyberbully his victim, or send vulgar e-mails to the victim's employer.[39] The victim suffers as a result of actions committed by the cyberharasser.[40]

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. The difference between cyberharassment and cyberstalking usually turns on a perpetrator's objective and motive for his behavior.[41] Cyberharassment is defined by a perpetrator's "desire to frighten or embarrass the harassment victim."[42] Cyberstalking is characterized as a perpetrator relentlessly pursuing his victim online, likely in combination with an offline attack.[43] Furthermore, a perpetrator's motive can distinguish whether an incident will qualify as cyberharassment or cyberstalking.[44] Cyberharassers often intend to teach their victims a lesson or solicit information from them, whereas cyberstalkers find purpose in revenge, anger, or obsession.[45]

Cyberbullying refers to "aggressive behavior that is intentional and involves an imbalance of power or strength" in electronic form.[46] Children and youths commit the majority of cyberbullying, which is characterized as aggressive behavior aimed to intimidate and induce fear in a victim.[47] It parallels cyberharassment in that both terms involve similar actions—both aim to frighten or

---

Frienster.com, About Friendster, http://www.friendster.com/info/index.php, (last visited Oct. 25, 2008).

38 Valetk, *supra* note 18.

39 *Id.*

40 *See id.* ("often, the victim is banned from bulletin boards, accused of improper conduct, and flooded with threatening messages.").

41 Parry Aftab, *Understanding the Cyberharassment Problem*, INFO. WEEK, Aug. 23, 2004, http://www.informationweek.com/story/showArticle.jhtml?articleID=29116706.

42 *Id.*

43 *Id.* There are three types of cyberharassment and cyberstalking situations: (1) "[o]nline cyberstalking and harassment that stays online;" (2) cyberharassment and cyberstalking that initiates online and either ventures offline or encourages a victim to go offline; and (3) "[o]ffline stalking or harassment that moves online." Wiredsafety.org, *Cyberstalking and Harassment FAQ*, http://www.wiredsafety.org/cyberstalking_harassment/csh6.html (last visited Sept. 8, 2008).

44 Aftab, *supra* note 41.

45 *See id.*

46 Stop Bullying Now!, What Adults Can Do, http://stopbullyingnow.hrsa.gov/adult/indexAdult.asp?Area=cyberbullying (last visited Sept. 8, 2008) ("Traditionally, bullying has involved actions such as hitting or punching (physical bullying), teasing or name-calling (verbal bullying), or intimidation through gestures or social exclusion.").

47 Cyberbullying most commonly occurs through instant message, chat rooms, e-mails, and messages posted on Web site bulletin boards. *Id.*

embarrass a victim and both involve posting private information about another person.[48] The main distinction between cyberbullying and cyberharassment has to do with age group; cyberbullying often refers to cyberharassment committed by children.[49]

Many state laws that address cyberharassment, cyberstalking, and cyberbullying combine the three types of cybercrimes in their statutory schemes.[50] Several federal legislative initiatives that address cyberharassment, cyberstalking, and cyberbullying use one term to encompass them all, despite the fact that the terms have different meanings.[51] The lack of a federal law intensifies the definitional problem.[52] Until Congress adopts a federal statute, the need for clearly stated definitions remains. For purposes of this Comment, the term cyberharassment will be used to encompass cyberstalking and cyberbullying.

B. Feasible and Anonymous: Internet Traits that Facilitate Cyberharassment

1. Anonymity in Cyberspace

The nature of the Internet allows information to flow freely and the marketplace of ideas to expand.[53] Contributing to the free flow is a person's ability to be and remain virtually anonymous.[54] Users can experiment with different personas, write a blog under a pseudonym,[55] or post comments on bulletin boards

---

48 Aftab, *supra* note 41. In a 2005 study, of those students who reported being cyberbullied at least twice in two months, 62% reported that they were cyberbullied by another student at school, 46% reported that they had been cyberbullied by a friend, and 55% reported not knowing who had cyberbullied them. Stop Bullying Now!, *supra* note 46.

49 *See* STOP Cyberbullying, *Telling the Difference Between Flaming, Cyber-Bullying and Harassment and Cyberstalking*, http://www.stopcyberbullying.org/pdf/telling_the_difference_le.pdf (last visited Aug. 22, 2008).

50 *See*, *e.g.*, *In re* Standard Jury Instructions in Criminal Cases, 953 So. 2d 495, 496 (Fla. 2007) (including the definition of harassment in cyberstalking). *See also* MO. REV. STAT. § 565.225.1(6) (2007).

51 *See* 1999 DOJ REPORT, *supra* note 26; *In re Standard Jury Instructions*, 953 So. 2d at 496–97.

52 *See* Aftab, *supra* note 41 ("While at least 46 states in the United States have various types of cyberstalking or harassment laws on the books, there is no U.S. federal cyberstalking or harassment law . . . ."); Valetk, *supra* note 18 ("Yet, despite the elusive, multijurisdictional nature of cyberstalking, no uniform federal law exists to protect victims or define ISP liability.").

53 *See* SOLOVE, *supra* note 30, at 17.

54 *See id.* at 139.

55 A blog created under a pseudonym does not include the blogger's real name or identity and retains the anonymity of the person blogging. *See* Harvey, *supra* note 37, at 2–3; *see also* SOLOVE, *supra* note 30, at 139 ("According to a [Pew Internet & American Life Project] survey, 55 percent of bloggers use pseudonyms rather than their real identities.").

without ever disclosing their identities.[56] Anonymity on the Internet thereby enhances traditional free speech and, in turn, promotes the concept of the marketplace of ideas.[57] It allows people to practice eccentricity without risking damage to their reputation.[58] Furthermore, anonymity on the Internet allows people to express their ideas and speak freely when they would otherwise fear to do so.[59] By increasing the opportunity for multiple ideas to exist simultaneously, the marketplace of ideas broadens. In theory, a greater number of ideas leads more quickly to societal truth.[60] According to scholar Daniel Solove, Internet anonymity "allows information to flow more freely than ever before. We can communicate and share ideas in unprecedented ways. These developments are revolutionizing our self-expression and enhancing our freedom."[61]

But at what price comes this enhanced freedom? The "revolutionizing" of our self-expression can result in extreme and undesirable forms of expression.[62] The Internet ensures one person's privacy to speak freely while also allowing an individual to invade the privacy of another. Essentially, the anonymity fostered by the Internet simultaneously preserves and undermines personal privacy.[63]

Anonymity on the Internet allows individuals to provide opinions and information that they might never otherwise divulge, including information that

---

56 SOLOVE, *supra* note 30, at 139.

57 *See id*. at 131, 140.

58 *Id.* at 140. This is not always the case, however. Anonymous eccentricity can, in fact, have drastic implications. When people disclose their identity on the Internet, the outcome is not always good. An example of such an instance is Jessica Cutler. As creator of the Washingtonienne blog, Jessica blogged about her sexual exploits, one of which was with Robert Steinbuch, a staff attorney for former U.S. Senator Mike DeWine. *Id.* at 50–52. When another popular Washington, D.C. blog linked to Jessica's blog, it received an exuberant number of hits. When Jessica attempted to delete her blog, it was already too late. She was exposed and had exposed third parties in her wake, including her sexual partners and her boss. *Id.* at 52–53. Although Jessica's tale is ultimately a success story—she exploited the attention garnering a book deal and a Playboy spread, her actions over the Internet resulted in the loss of her job and the exposure of those who never sought an interactive outlet. *Id.* at 54.

59 *Id.* at 140 ("Without anonymity, some people might not be wiling to express controversial ideas.").

60 *See* Abrams v. United States, 250 U.S. 616, 630 (1919) (Holmes, J. dissenting). Justice Holmes articulated the market place of ideas concept in his dissent:

> [W]hen men have realized that time has upset many fighting faiths, they may come to believe even more than they believe the very foundations of their own conduct that the ultimate good desired is better reached by free trade in ideas—that the best test of truth is the power of the thought to get itself accepted in the competition of the market, and that truth is the only ground upon which their wishes safely can be carried out.

Id.

61 SOLOVE, *supra* note 30, at 17.

62 *See* Harvey, *supra* note 37 (noting that anonymity appeals to harassers).

63 SOLOVE, *supra* note 30, at 141 ("[A]nonymity is a form of privacy protection, yet it can also facilitate privacy violations.").

is false and harmful to third parties.[64] As Solove observed in *The Future of Reputation: Gossip, Rumor, and Privacy on the Internet*: "When people are less accountable for their conduct, they are more likely to engage in unsavory acts. When anonymous, people are often much nastier and more uncivil in their speech. It is easier to say harmful things about others when we don't have to take responsibility."[65] Due to the easy accessibility and usability of the Internet, not only can anonymous individuals partake in "unsavory acts," but groups can also form against a single target and threaten that person's reputation or personal safety.[66]

Long settled law confirms that the First Amendment protects the right to speak anonymously.[67] In *McIntyre v. Ohio Elections Commission*, the Supreme Court held that First Amendment protection extends to a writer's decision to speak anonymously: "Anonymity is a shield from the tyranny of the majority. It thus exemplifies the purpose behind the Bill of Rights, and of the First Amendment in particular: to protect unpopular individuals from retaliation . . . at the hand of an intolerant society."[68] Accordingly, the constitutional right to speak anonymously is vigilantly safeguarded.[69] However, when anonymity is used as an advantage to defame and hurt a person in cyberspace, it should not be similarly protected. A benefit of technological advancement is the ability to pierce the veil of anonymity if the law requires it.

One dimension of anonymity on the Internet is traceability.[70] Current technology allows otherwise anonymous users to be traced, which ultimately leads to discovery of the user's identity.[71] Tracing a cyberharasser is one method through which a victim could seek remedy. Additionally, Congress could draft a federal law that distinguishes between lawful and unlawful anonymity on the Internet. Solove stated that "the key is for the law to allow the unmasking of anonymous people when they engage in harmful speech about others."[72] However, the standard for when to trace an anonymous cyberharasser must be high

---

64 *See* Harvey, *supra* note 37, at 3; SOLOVE, *supra* note 30, at 140.

65 SOLOVE, *supra* note 30, at 140.

66 *Id.* On the day of her suicide, the same harassment that Megan Meier sought to avoid when she transferred middle schools targeted her once again when she was "hounded and publicly humiliated by a teenage mob on the Web, set upon in a virtual Lord of the Cyberflies." Jones, *supra* note 5.

67 *See* Talley v. California, 362 U.S. 60, 64 (1960) ("Anonymous pamphlets, leaflets, brochures and even books have played an important role in the progress of mankind.").

68 McIntyre v. Ohio Election Comm'n., 514 U.S. 334, 357 (1995) (citation omitted).

69 *See id.*

70 SOLOVE, *supra* note 30, at 146.

71 *Id.* at 146–47. An Internet Protocol ("IP") address can be used to trace an anonymous user on the Internet. Whenever people communicate over the Internet, their IP addresses are logged with their ISP. The ISP can then, if needed, trace the IP address back to the user. *Id.* at 147.

72 *Id.* at 147.

in order to not only avoid bad-faith lawsuits, but also to keep intact anonymity that facilitates the exchange of ideas.[73]

2. An Invasion of Privacy

Both anonymity and feasibility enabled by the Internet create a challenge to the traditional understanding of privacy law.[74] Traditionally, the concept of privacy is twofold: people cannot expect privacy if they are in public places, even when they believe their acts are private.[75] Courts determine whether an incident is private by applying the tort of public disclosure: "There is no liability when the defendant merely gives further publicity to information about the plaintiff [that] is already public. Thus there is no liability for giving publicity to facts about the plaintiff's life that are matters of public record . . . ."[76]

Today, information never intended to be public is exposed via the Internet.[77] The nature of the exposure not only invades an individual's expectation of privacy, but it also calls into question the traditional definition of privacy.[78] What otherwise would be a fleeting memory in the minds of a few bystanders can now be posted on the Internet and scrutinized extensively and continuously.[79] In turn, this scrutiny can rise to the level of cyberharassment.

An example of such an incident involved "*gae-ttong-nyue*," roughly translated as "dog-shit-girl."[80] A young woman's small dog defecated on a subway train in South Korea.[81] When other passengers asked her to clean the mess up, she told them to mind their own business.[82] An enraged passenger nearby took pictures of her and posted the pictures on a popular Korean blog.[83] Within

---

[73] *Id.* at 149.

[74] *Id.* at 163 (explaining that traditional privacy law was "binary," focusing on two "realms," public and private, and that modern technology "poses a severe" challenge to the binary framework).

[75] Gill v. Hearst Pub. Co., 253 P.2d 441, 444 (Cal. 1953) (stating that where a couple, who had engaged in a romantic embrace that was later published in an issue of *Harper's Bazaar* "had voluntarily exposed themselves to public gaze in a pose open to the view of any persons who might then be at or near their place of business . . . . There can be no privacy in that which is already public." (citation omitted) (internal quotation marks omitted)).

[76] RESTATEMENT (SECOND) OF TORTS § 652D cmt. b (1977).

[77] *See* SOLOVE, *supra* note 30, at 164.

[78] *Id.* at 164–65 ("We often engage in our daily activities in public expecting to be just a face in the crowd, another ant in the colony.").

[79] Andrew Jay McClurg, *Bringing Privacy Law Out of the Closet: A Tort Theory of Liability for Intrusions in Public Places*, 73 N.C. L. REV. 989, 1041–42 (1995).

[80] Don Park's Daily Habit, *Korean Netizens Attack Dog-Shit-Girl*, http://www.docuverse.com/blog/donpark/2005/06/08/korean-netizens-attack-dog-shit-girl (June 8, 2005, 5:59 EST) (this blog is being migrated to http://donpark.wordpress.com/).

[81] *Id.*

[82] SOLOVE, *supra* note 30, at 1; *see also* Don Park's Daily Habit, *supra* note 80.

[83] SOLOVE, *supra* note 30, at 1; *see also* Don Park's Daily Habit, *supra* note 80.

hours, bloggers labeled her as dog-shit-girl and spread her picture across cyberspace.[84] They exposed her identity, and others sought information on her parents and relatives.[85] The story became a national news story in Korea, and her reputation eventually spread as far as the United States.[86] As a result of the harassment she suffered, the woman dropped out of her university.[87]

Under the traditional view of privacy, dog-shit-girl could expect no privacy because she was in public.[88] Her dog defecated on a public train and her actions following the act were public. However, once another passenger took her picture, the incident was taken out of context.[89] The nature of the Web allowed the story to become a widespread headline.[90] But for the photo being posted on the Internet, the event likely would have been an ephemeral memory of her fellow passengers.[91] The incident was a public one; however, the woman's public presence did not give others the right to photograph, ridicule, and post her private information on the Internet.

As exhibited by the dog-shit-girl scenario, the expansion of modern technology blurs the line of understanding between what is considered public and private information.[92] With a cell phone, a person can hold a private phone conversation in a public place.[93] People also have private conversations in public that they do not expect or want third parties to hear.[94] Modern society's notion of privacy involves more than the idea that an act executed in public is not private.[95] Moreover, as in the case of dog-shit-girl, the question arises as to whether the law protects the exposure of private information related to a public

---

84 Don Park's Daily Habit, *supra* note 80.

85 *Id.*

86 *See* SOLOVE, *supra* note 30, at 1 (noting that the posting of the story on Don Park's blog spread the story to the United States).

87 Jonathan Krim, *Subway Fracas Escalates into Test of the Internet's Power to Shame*, WASH. POST, July 7, 2005, at D1.

88 Posting of Chuck to Don Park's Daily Habit, Comments, *Korean Netizens Attack Dog-Shit-Girl*, http://www.docuverse.com/blog/donpark/2005/06/08/korean-netizens-attack-dog-shit-girl (June 29, 2005, 13:24 EST) (exemplifying the sentiment that dog-shit-girl could not expect privacy because she was in public: "The initial blogger. Do I think he had every right to post her? Yep. She was in public, and it really doesn't matter if she was in front of 100 or 1,000,000 people, she was willing to act that way in the public sphere.").

89 Helen Nissenbaum, *Privacy as Contextual Integrity*, 79 WASH. L. REV. 119, 144–45 (2004) (discussing "contextual integrity" as a construct to view privacy violations in relation to the technology used to commit the violation—if the technology is common, the violation is less intrusive).

90 SOLOVE, *supra* note 30, at 8.

91 *Id.*

92 *Id.* at 7–9, 166.

93 *Id.* at 166.

94 *See id.* (asserting that if an individual has a cell phone conversation on a train, despite the fact that other passengers might overhear the conversation, the individual expects a certain level of privacy—that the conversation not be recorded and rebroadcast).

95 *See id.*

act.[96] New technologies increasingly impede upon the privacy and relative safety that many people enjoy in a public setting. The traditional test to determine whether or not something is private can no longer depend on the basis of whether information is publicly exposed.[97]

III. INCIDENTS OF CYBERHARASSMENT: INTENTIONAL AND UNINTENTIONAL

As the Internet continues to assert its presence in the lives of Americans, the exposure of personal information on the Internet increases while online safe harbors decrease. Exposure can be either intentional or unintentional. In either case, actions that victimize a person or expose her personal information can qualify as cyberharassment. The following examples demonstrate intentional and unintentional cyberharassment.

A. Intentional Cyberharassment: Ryan Halligan

Three years before the suicide of Megan Meier, a thirteen-year-old boy named Ryan Halligan committed suicide following months of online harassment by his peers.[98] After suffering from harassment in school during the day, Ryan returned home to a barrage of instant messages from classmates insinuating he was gay.[99] Both in school and at home, he was the victim of intense harassment; the only difference was the mode of the harassment.[100] Consequently, Ryan had no offline or online safe harbor.

A few days after Ryan's funeral, his father logged onto his AOL IM account to investigate Ryan's suicide.[101] Ryan's father stated, "It was in that safe world of being somewhat anonymous that several of his classmates told me of the bullying and cyberbullying that took place during the months that led up to [Ryan's] suicide."[102] His father:

> [D]iscovered a folder filled with IM exchanges . . . and further interviewed his classmates, [and] realized that technology was being utilized as [a weapon] far more effective and reaching than the simple ones [he] had as [a kid]. Passing handwritten notes

---

96 *See* SOLOVE, *supra* note 30, at 7–9.

97 *Id.* at 166.

98 RyanPatrickHalligan.org, *In Memory of Ryan Patrick Halligan*, http://www.ryanpatrickhalligan.org/ (last visited Sept. 1, 2008).

99 *See id.* ("Thus merely assessing whether information is exposed in public or to others can no longer be adequate to determining whether we should protect it as private.").

100 *See id.*; *see also* Associated Press, *States Pushing for Laws to Curb Cyberbullying* FOXNEWS.COM, Feb. 21, 2007, http://www.foxnews.com/story/0,2933,253259,00.html [hereinafter *Laws to Curb Cyberbullying*].

101 *See In Memory of Ryan Patrick Halligan*, *supra* note 98.

102 *Id.*

> or a "slam" book has since been replaced with on-line tools such as IM, Web sites, Blogs, cell phones, etc. The list keeps growing with the invention of every new hi-tech communication gadget.[103]

Mr. Halligan concluded that harassment through technology magnifies and amplifies a person's hurt feelings,[104] which, as illustrated by the cases of his son Ryan and Megan Meier, can encourage teen suicide.[105] Mr. Halligan determined that his son suffered from depression amplified by a steady onslaught of electronic harassment.[106] The Internet did not cause Ryan's death, but it served as an accelerator of his pain.[107]

Ryan's case illustrates the intentional form of cyberharassment. Over five years following Ryan's death, legislatures continue to disagree on how to properly police cyberharassment.[108] The increase in cyberharassment may force many legislatures to take action.[109] However, even if states enact laws addressing cyberharassment, the laws may be ineffective, because harassment involves a societal norm that cannot be legislated; rather, effective deterrence of harassment requires education.[110] Furthermore, the lack of cyberharassment legislation most likely is due to challenges in drafting the legislation without infringing on free speech rights.[111] Specifically, legislatures have yet to agree upon the proper balance between an individual's right to express himself and simultaneously keep his safety and privacy intact.[112]

---

[103] *Id.*

[104] Felicia R. Lee, *The Rough-and-Tumble Online Universe Traversed by Young Cybernauts*, N.Y. TIMES, Jan. 22, 2008, at E1. *See also Laws to Curb Cyberbullying*, *supra* note 100 ("The Internet allows students to insult others in relative anonymity, and experts who study cyberbullying say it can be more damaging to victims than traditional bullying like fist fights and classroom taunts.").

[105] *See*, *e.g.*, *Laws to Curb Cyberbullying*, *supra* note 100 (noting that 13-year-old Ryan Halligan's suicide was caused by continuous Internet harassment); Blank, *supra* note 27 (explaining 13-year-old Megan Meier committed suicide after receiving continuous insults via the computer).

[106] Abbott Koloff, *States Push for Cyberbully Controls*, USA TODAY, Feb. 7, 2008, at 3A.

[107] *Id.*

[108] *See infra* Part V; *Laws to Curb Cyberbullying*, *supra* note 100 ("States from Oregon to Rhode Island are considering crackdowns to curb or outlaw the behavior . . . .").

[109] In response to Ryan's suicide, the Vermont legislature passed an anti-cyberbullying law. It required schools to regulate bullying both on and off of school grounds and included bullying over the Internet. VT. STAT. ANN. tit. 16, § 1161a(a)(6) (2007). Rhode Island State Senator John Tassoni, who introduced a bill to study cyberbullying, stated, "The kids are forcing our hands to do something legislatively." *Laws to Curb Cyberbullying*, *supra* note 100.

[110] *Laws to Curb Cyberbullying*, *supra* note 100. George McDonough, an education coordinator with Rhode Island's Department of Education, stated, "You can't legislate norms, you can only teach norms. Just because it's a law they don't necessarily follow it. I mean, look at the speed limit." *Id.*

[111] *See* Koloff, *supra* note 106; *Laws to Curb Cyberbullying*, *supra* note 100.

[112] *See* Koloff, *supra* note 106.

B. Unintentional Cyberharassment: Star Wars Kid

In April 2003, Quebec teenager Ghyslian Raza became the target of "worldwide mockery" when his classmates posted a self-made video of him practicing his light saber moves on an Internet file-sharing network.[113] The fourteen-year-old filmed himself for two minutes fighting a mock battle with a golf ball retriever, even generating his own sound effects while pretending to be a character from the movie *Star Wars: Episode I, The Phantom Menace*.[114] Apparently, he did not intend the video for public consumption.[115] However, approximately six months later, his classmates discovered it on a shelf of his school's TV studio[116] and posted it online where it became an instant phenomenon.[117] Internet users from around the world downloaded the video more than a million times and nicknamed Ghyslian "Star Wars Kid."[118] Bloggers created remix versions of the video, adding sound and lighting effects.[119] The mainstream media discovered the story, and soon enough, published Ghyslian's story in newspapers such as the *New York Times*.[120]

As a result of his newfound popularity, Ghyslian became the victim of severe harassment by people who posted defamatory comments about him on the Web.[121] Ghyslian transferred to another high school to avoid severe tormenting by his classmates, but dropped out of his new school when the harassment did not cease.[122] Ghyslian's parents sued his classmates who posted the video online, claiming that "Ghyslain had to endure, and still endures today, harass-

---

113 *Star Wars Kid Files Lawsuit*, WIRED.COM, June 24, 2003, http://www.wired.com/culture/lifestyle/news/2003/07/59757 (last visited Mar. 18, 2008).

114 *Id.*; Tu Thanh Ha, "*Star Wars Kid" Cuts a Deal with His Tormentors*, GLOBE & MAIL, Apr. 7, 2006, at A8, *available at* http://www.theglobeandmail.com/servlet/story/RTGAM.20060407.gtstarwars07/BNStory/National/; Amy Harmon, *Fame Is No Laughing Matter for the "Star Wars Kid*," N.Y. TIMES, May 19, 2003 at C3.

115 *Star Wars Kid Files Lawsuit*, *supra* note 113.

116 Tu Thanh Ha, *supra* note 114. The fact that Ghyslian left the video on a shelf at his school where anyone could access it raises questions about whether he assumed the risk that someone might discover the tape and post it on the Internet. However, an incident like Ghyslian's does not give another person the right to invade one's expectation of privacy. If an assumption of the risk defense were to survive, it would result in paranoia of people like Ghyslian to enter the public sphere.

117 *See* Harmon, *supra* note 114.

118 *See* Tu Thanh Ha, *supra* note 114.

119 *See* SOLOVE, *supra* note 30, at 45–46; *see also*, Harmon, *supra* note 114.

120 *See*, *e.g.*, Harmon, *supra* note 114. ("Short videos of embarrassing, funny or illicit moments are common Internet fare. But this one, known as the Star Wars Kid, has traveled farther, faster and commanded more attention than any in recent memory. It seems to be serving as a Rorschach test for geek self-perception.").

121 *See*, *e.g.*, WAXY.ORG, *Star Wars Kid*, Apr. 29, 2003, http://www.waxy.org/archive/2003/04/29/star_war.shtml; *see also* Harmon, *supra* note 114.

122 *See*, *e.g.*, Harmon, *supra* note 114.

ment and derision from his high-school mates and the public at large."[123] The case eventually settled; however, the psychiatric damage and emotional distress had already affected Ghyslain.[124]

The aftermath of Ghyslain's unintended event will forever dub him as "Star Wars Kid."[125] Years later, the video remains viewable and the subject of comment by journalists and bloggers.[126] Nothing prohibited Ghyslain's classmates from obtaining the video and posting it on the Web site of their choosing. Although most likely unintentional, their actions caused a severe invasion of Ghyslain's privacy.[127]

One could argue that by posting the video, Ghyslain's classmates had the intention to harass him via the Web. One could also argue that the millions of viewers and those who parodied the video had the same intentions. However, more likely, the viewers saw the video as purely a form of entertainment; they likely thought only that the video made them laugh and that it would make others laugh as well. His classmates likely failed to consider the risk to Ghyslain's reputation and privacy or the possibility of worldwide harassment of Ghyslain. Also, his classmates likely were unaware of the possible illegality of such a prank. The Star Wars Kid incident illustrates the challenging implications for harassment, which increase as our privacy continues to be compromised through the Web.[128]

IV. FEDERAL LAW AND COMMENTARY RELATED TO CYBERHARASSMENT

Traditional, federal harassment statutes focus on physical contact between the harasser and the victim and therefore inappropriately address the virtual nature of cyberharassment.[129] Although Congress has enacted legislation to

---

123 *Star Wars Kid Files Lawsuit*, supra note 113.

124 *See id.* ("Ghyslain's parents claim their son was so humiliated, he is undergoing psychiatric care and may be marked for life by the experience."); SOLOVE, *supra* note 30, at 47 (noting that Ghyslain was "deeply scarred by the incident"). Suing a known cyberharasser can qualify as a potential remedy for victims. However, where there is intentional infliction of emotional distress so extreme that a person must seek psychiatric help, medication, etc., greater punishment is necessary.

125 SOLOVE, *supra* note 30, at 47 ("Forever, Ghyslain will be known as the Star Wars Kid.").

126 *See id.* (noting that the video is estimated as the most watched video on the Internet).

127 *See id.* at 45–47 (explaining the video was an unintentional Internet sensation and ultimately had a significant negative impact on Ghyslain's life).

128 *See id.* at 47–48.

129 *See* 47 U.S.C. § 223(a) (2000) (prohibiting use of a telephone or telecommunications device to annoy, abuse, harass, or threaten any person at the number called); 18 U.S.C. § 875 (2006) (covering threats and harassment).

protect children on the Internet, mainly from harmful content,[130] enacting legislation to protect victims from harassers on the Internet has not been a congressional priority.[131] Victims of cyberharassment are limited to civil litigation as a remedy: victims can sue for defamation, invasion of privacy, or intentional infliction of emotional distress.[132] Victims might also find recourse by reporting a cyberharasser to an ISP and then attempting to sue the ISP itself under section 509 of the CDA.[133] However, when utilized in suits for unlawful conduct over the Internet, these options are increasingly restricted and leave victims of cyberharassment ineffectively protected.[134] Fortunately, Congress has started to recognize the increasing problems caused by cyberharassment.[135]

A. Traditional Defamation Law

Victims of cyberharassment may pursue civil action against cyberharassers for circulation of information or misinformation under the tort of defamation.[136] The effectiveness of a defamation suit, however, is questionable. Defamation law attempts to protect against various types of reputation libel and slander,[137]

---

130 *See* Children's Internet Protection Act, Pub. L. No. 106-544, tit. XVII, 114 Stat. 2763A-335 (2000); Adam Walsh Child Protection and Safety Act of 2006, Pub. L. No. 109-248, 120 Stat. 587.

131 *But see* ADAM THIERER, CONGRESS CONTENT REGULATION, AND CHILD PROTECTION: THE EXPANDING LEGISLATIVE AGENDA, PROGRESS & FREEDOM FOUND., PROGRESS SNAPSHOT 4.4 at 1, (2008), *available at* http://pff.org/issues-pubs/ps/2008/ps4.4childprotection.html (illustrating the "explosion of legislative proposals dealing with online child safety" in the 110th session of Congress).

132 *See infra* Part IV.A (explaining the applicability of traditional defamation law to cyberharassment); Aftab, *supra* note 41 ("Often the victims of cyberstalking and cyberharassment are limited to civil litigation . . . .").

133 Communications Decency Act of 1996, Pub. L. No. 104-104, sec. 509, § 223, 110 Stat. 137 (codified as amended at 47 U.S.C. § 230 (2000)).

134 *See* Universal Commc'n Sys., Inc. v. Lycos, Inc., 478 F.3d 413, 419–22 (1st Cir. 2007) (finding very narrow liability for ISPs under the Communications Decency Act). *See generally* Zeran v. America Online, Inc., 129 F.3d 327 (4th Cir. 1997) (finding America Online to be a publisher under the Communication Decency Act and therefore, immune from a defamation suit).

135 *See infra* Part IV.C (explaining recent governmental recognition of the cyberharassment problem). *See generally* 1999 DOJ REPORT, *supra* note 26 (regarding the challenge of cyberstalking to government and industry).

136 SOLOVE, *supra* note 30, at 113.

137 Slander consists of "ephemeral communications such as the speech, gestures, and sign language"; while libel refers to "defamatory communications of a more or less permanent sort such as printed matter, films, and art work." William J. Andrle, Jr., *Extension of Absolute Privilege to Defamation in Arbitration Proceedings:* Sturdivant v. Seaboard Service System, Ltd., CATHOLIC U. L. REV. 1073, 1073 n.1 (1984); *see* RESTATEMENT (SECOND) OF TORTS §§ 568, 559 (1977); Russ VerSteeg, *Slander & Slander Damages after* Gertz *and* Dun & Bradstreet, 38 VILL. L. REV. 655, 659–660 (1993).

including "reputation as property, as honor, and as dignity."[138] Most harassing communication over the Internet qualifies as libel since it is in print form.[139] In order to succeed in a defamation lawsuit, a plaintiff must meet six elements that comprise a libel claim.[140] As defined in *New York Times Co. v. Sullivan*, a plaintiff must exhibit: (1) a defamatory communication; (2) a false statement of fact; (3) publication of the false message to a third person; (4) identification of the plaintiff; (5) depending on the private or public nature of the plaintiff, fault on the part of the libeler through either negligence or actual malice; and (6) that the defamation caused injury or harm to the plaintiff.[141] A successful plaintiff in a defamation suit necessarily trumps any First Amendment rights asserted by a defendant.[142] However, free speech protection occasionally outweighs an individual's right to protection from harassment.

The Supreme Court addressed this issue and considered the balance between protecting free speech and allowing redress for defamatory statements in *New York Times*.[143] The law only protects a person from the dissemination of false and reputation damaging information.[144] Defamation law does not protect individuals from being the target of harassment, which can include negative opinions, criticism, and insults.[145] The power of the Internet increases the opportunity for free speech, but with this opportunity comes the potential for increased abuse: "In cyberspace, the power to defame is unprecedented."[146] Furthermore, Congress intended to encourage self-policing by Internet users and Web site operators in order to further expand free speech and the marketplace of ideas in enacting the Telecommunications Act of 1996.[147] Essentially, the privacy of an individual on the Internet is valued less than her ability to speak freely.

---

[138] Robert C. Post, *The Social Foundations of Defamation Law: Reputation and the Constitution*, 74 CAL. L. REV. 691, 693 (1986).

[139] RESTATEMENT (SECOND) OF TORTS § 559 (defining defamatory communication). With respect to defamation, the Restatement defines "communication" broadly as "the fact that one person has brought an idea to the perception of another." *Id.* cmt. A.

[140] *See generally* N.Y. Times Co. v. Sullivan, 376 U.S. 254 (1964) (enunciating the elements of a libel claim).

[141] *See* RESTATEMENT (SECOND) OF TORTS § 558; *N.Y. Times Co.*, 376 U.S. at 280–81.

[142] *See N.Y. Times Co.*, 376 U.S. at 279–83 (finding that in some instances, the benefits of a citizen's ability to criticize public officials without recourse outweigh the official's right to be free from defamation.).

[143] *See id.*; SOLOVE, *supra* note 30, at 118, 126.

[144] RESTATEMENT (SECOND) OF TORTS §§ 559, 568. Under the Restatement, a defamatory statement does not have to cause actual harm to an individual's reputation, rather liability depends on the tendency of the communication to have such an effect. § 559 cmt. d.

[145] SOLOVE, *supra* note 30, at 120.

[146] Bruce W. Sanford & Michael J. Loenger, *Teaching an Old Dog New Tricks: The First Amendment in an Online World*, 28 CONN. L. REV. 1137, 1154 (1996).

[147] *See* 47 U.S.C. § 230(a) (2000) (explaining that the Internet "offer[s] a forum for true diversity of political discourse" and that the services on the Internet allow "users a great degree of control over the information they receive").

Although traditional defamation law may be applied to the Internet and cyberharassment, the current law is inadequate for numerous reasons. First, the likelihood of a plaintiff succeeding in meeting each prong of a libel claim is slim. The voluntary nature of the Internet makes it difficult for a plaintiff to rebut a defendant's standard defense—that a victim assumes the risk of harassment when she subjects herself to defamation on the Internet.[148] If a victim of cyberharassment claims that her harasser intentionally or recklessly caused severe emotional distress, the claim would likely fail due to the heavy burden a plaintiff carries to show clear-cut proof of the defendant's state of mind.[149] Moreover, application of traditional defamation law to the Internet is difficult because more often than not, plaintiffs do not know the identity of their defamers or harassers. Additionally, because of the Internet's anonymous nature, plaintiffs who think they know the identity of their harasser could be wrong. The Megan Meier story exemplifies such a case, and a similar situation could result in a suit against the wrong person. John Doe lawsuits, which do not initially identify the cyberharasser by name, are "one of [the] few weapons against what [persons and corporations] consider digital defamation."[150] As new technologies expand the range of the means of defamation, the targets of Internet harassment will find it increasingly difficult to prove defamation using the traditional test.

B. Communications Decency Act

In an effort to stimulate competition in the telecommunications field and outlaw use of computers and phone lines to transmit indecent material, Congress passed the Telecommunications Act of 1996 ("the 1996 Act").[151] Title V

---

[148] Sanford & Loenger, *supra* note 146, at 1158.

[149] To establish a claim of intentional infliction of emotional distress, a plaintiff must show: 1) the defendant acted intentionally or recklessly; 2) the defendant's conduct was extreme and outrageous; and 3) the conduct was the cause 4) of severe emotional distress. Allen v. Allison, 155 S.W.3d 682, 691 (Ark. 2004); *see also* 86 C.J.S. *Torts* § 70 (2000) ("One who by extreme and outrageous conduct intentionally or recklessly causes severe emotional distress to another is subject to liability for such emotional distress and for bodily harm resulting from the distress.").

[150] Greg Miller, *"John Doe" Suits Threaten Internet Users' Anonymity*, L.A. TIMES, June 14, 1999, at A1. John Doe lawsuits are used by plaintiffs in defamation suits when they do not know who their defamers are, usually in cases involving defamation over the Internet. *See id.*

[151] Telecommunications Act of 1996, Pub. L. No. 104-104, 110 Stat. 56 ("To promote competition and reduce regulation in order to secure lower prices and higher quality service for American telecommunications . . . ."); *id.* sec. 502, § 223 (amending 47 U.S.C. § 223) (making transmission of obscene material via telephone or computer punishable by fine or imprisonment); *see also* Thomas W. Hazlett & David W. Sosa, *"Chilling" the Internet? Lessons from FCC Regulation of Radio Broadcasting*, 4 MICH. TELECOMM. & TECH. L. REV.

of the Act was codified as the Communications Decency Act.[152] Congress enacted the CDA to support and promote the dissemination of information on the Internet, while protecting minors from indecent content on the Internet.[153] Section 230 of the 1996 Act explains that "[n]o 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."[154] Section 230 protects any provider or user of an interactive computer service that restricts access to, or availability of, material the provider or user believes to be indecent from liability for defamatory content.[155] By classifying ISPs[156] and hosts of online forums as publishers or distributors of content, the CDA immunized them from liability for defamatory content submitted by their users.[157] Congress reasoned that holding ISPs liable for the actions of its subscribers was too great a threat

---

35 (1998) (noting that the CDA was signed into law as part of the 1996 Act).

[152] Telecommunications Act of 1996, tit. V.

[153] 47 U.S.C. § 230(b) (2000). The Communications Decency Act was enacted, in part, "to preserve the vibrant and competitive free market that presently exists for the Internet and other interactive computer services," and to promote the free market concept best achieved with minimal government regulation. *Id.*

[154] Telecommunication Act of 1996 § 509(c)(1), 47 U.S.C. § 230(c)(1) (2000). Section 230 was enacted specifically

> [T]o overrule *Stratton-Oakmont v. Prodigy* and any other similar decisions which have treated such providers and users as publishers or speakers of content that is not their own because they have restricted access to objectionable material. The conferees believe that such decisions create serious obstacles to the important federal policy of empowering parents to determine the content of communications their children receive through interactive computer services.

H.R. REP. NO. 104-458, at 194 (1996) (Conf. Rep.) *reprinted in* 1996 U.S.C.C.A.N. 10, 208.

[155] § 230(c). The relevant portion of the statute provides

> (2) Civil liability
>
> No provider or user of an interactive computer service shall be held liable on account of—
>
> (A) any action voluntarily taken in good faith to restrict access to or availability of material that the provider or user considers to be obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable, whether or not such material is constitutionally protected; or
>
> (B) any action taken to enable or make available to information content providers or others the technical means to restrict access to material described in paragraph (1).

Id.

[156] The statute defines an ISP as an "interactive computer service," i.e., "any information service, system, or access software provider that provides or enables computer access by multiple users to a computer server, including specifically a service or system that provides access to the Internet and such systems operated or services offered by libraries or educational institutions." § 230(f)(2). Furthermore, the statute defines an "information content provider" as "any person or entity that is responsible, in whole or in part, for the creation or development of information provided through the Internet or any other interactive computer service." § 230(f)(3).

[157] *See* SOLOVE, *supra* note 30, at 152.

to free speech.[158] The blanket immunity provided by section 230 was intended to serve various public interests.[159] For example, Congress wanted ISPs to be able to self-regulate, promote the free exchange of information, and further advance growth of the Internet.[160]

However, in retrospect, the law may not be serving the public interest as Congress intended. Numerous court decisions upholding ISP immunity under section 230 demonstrate that the statute is overly broad, or at a minimum, the statute has been interpreted unnecessarily broadly by the courts.[161] Individuals subjected to extreme online harassment appear to have no claim under section 230 because the medium of their harassment is immune from liability.[162] Yet clause (b) of section 230 explicitly states that "[i]t is the policy of the United States . . . to ensure vigorous enforcement of Federal criminal laws to deter and punish trafficking in obscenity, stalking, and harassment by means of computer."[163] Nonetheless, this policy has not been enforced or has been overlooked. Courts have found ISPs immune from liability for any kind of defamatory comments posted by their users, including those of a stalking or harassing nature. Part of Congress's reasoning for enacting section 230 was to protect minors from offensive content.[164]

A summary of relevant case law illustrates this point. In the first post-CDA decision in 1997, *Zeran v. America Online, Inc.*, the United States Court of Appeals for the Fourth Circuit ("Fourth Circuit") interpreted section 230 as removing publisher and distributor liability for Internet communication forums despite the extreme online harassment suffered by the petitioner, Kenneth Zeran.[165]

About a week after the 1995 Oklahoma City bombing, Zeran had his phone number anonymously posted in an advertisement on an AOL bulletin board.[166] The advertisement offered T-shirts for purchase with distasteful slogans about the Oklahoma City bombing.[167] The message stated that interested people

---

158 *Id.*

159 § 230(b) (listing five policies supported by the immunity provided to ISPs).

160 § 230(b)(1)–(4).

161 *See* Universal Commc'n Sys., Inc. v. Lycos, Inc., 478 F.3d 413 (1st Cir. 2007) (holding that "under Communications Decency Act[,] Internet message board operator was immune from liability for allegedly false and defamatory postings made by third party subscribers."); s*ee also* Zeran v. Am. Online, Inc., 129 F.3d 327, 328 (4th Cir. 1997) ("Section 230 . . . plainly immunizes computer service providers . . . from liability for information that originates with third parties.").

162 § 230(c). *See Lycos*, 478 F.3d at 413; *Zeran*, 129 F.3d at 328.

163 § 230(b)(5).

164 § 230(b).

165 *See generally Zeran*, 129 F.3d at 327.

166 *Id.* at 329 (explaining that the posting was entitled "Naughty Oklahoma T-Shirts").

167 *Id.*

should call "Ken" and listed Zeran's phone number as the contact.[168] However, Zeran had not posted the advertisement.[169] He learned about the posting when he began receiving harassing phone calls from angered Oklahomans threatening violence or death.[170] The phone calls became constant, with Zeran receiving threats approximately every two minutes.[171] Zeran called AOL to demand that the posting be removed and that a retraction be posted.[172] AOL agreed to remove the posting but declined to post a retraction.[173] The calls to Zeran's house continued, and he discovered that there was a second posting stating new T-shirts were available with new slogans.[174] Furthermore, the new posting said that callers should ask for "Ken" and to "please call back if busy."[175] The calls continued despite Zeran's additional calls to AOL demanding that the posting be taken down.[176] Zeran's position worsened when a local radio station discovered the posting and the broadcaster encouraged listeners to call Zeran and express their outrage.[177] The situation escalated to the point that Zeran needed police to monitor his house.[178] Once the mainstream media reported the inaccuracy of the advertisement, the calls subsided. However, Zeran was so disturbed by the ordeal that he had started taking anti-anxiety medication.[179]

Zeran sued AOL, claiming that the service provider unreasonably delayed its removal of the defamatory postings.[180] The Fourth Circuit cited section 230 and explained that the statute created immunity against any action which seeks to impose ISP liability for a third party posting.[181] The Court went on to explain the congressional intent behind enactment of section 230:

> The purpose of this statutory immunity is not difficult to discern. Congress recognized

---

168 *See id.*

169 *See Zeran*, 129 F.3d at 329 (explaining that an "unidentified person" posted the advertisement and describing it as an "anonymously perpetrated prank").

170 *Id.*

171 *Id.*

172 *Id.*

173 *Id.*

174 *Id.*

175 *Id.* Zeran ran a business out of his home, for which he gave out his phone number. Because he did not want to hurt his business, he did not change his phone number. *Id.*

176 *Id.* Zeran was told that "the individual account from which the messages were posted would soon be closed." *Id.* Zeran also reported the cases to the Federal Bureau of Investigation office in Seattle, Washington. *Id.*

177 *Id.*

178 *Id.*

179 *Id.*

180 *Id.* He did not bring any action against the party who posted the messages, claiming that AOL made it impossible to identify the original defamer because it neglected to keep adequate records of its users. *Id.* at 329 n.1.

181 *Id.* at 330. The court explained that the operation of section 230 "precludes courts from entertaining claims that would place a computer service provider in a publisher's role." *Id.*

> the threat that tort-based lawsuits pose to freedom of speech in the new and burgeoning Internet medium. The imposition of tort liability on service providers or the communications of others represented, for Congress, simply another form of intrusive government regulation of speech. Section 230 was enacted, in part, to maintain the robust nature of Internet communication and, accordingly, to keep government interference in the medium to a minimum . . . . Congress further stated that it is the policy of the United States . . . to preserve the vibrant and competitive free market that presently exists for the Internet and other interactive computer services, *unfettered by Federal or State regulation*.[182]

Opponents of Internet regulation argue that creating immunity for service providers is important because it prevents the chilling of speech that might result otherwise. They argue that expecting a service provider to monitor and filter out each defamatory comment or complaint is unrealistic.

As a result of section 230's broad immunity, however, a victim of harassment like Zeran is left with limited legal options. Zeran's case exemplifies an overly broad interpretation of section 230 and provides too much immunity for service providers, thereby failing to balance properly speech and privacy.[183] Zeran's right to privacy was violated in order to promote the right of free speech. The problem has only worsened over the years, as Web sites created purely for the purpose of spreading gossip and rumors have proliferated.[184] Despite the fact that these sites result in an extreme violation of a person's privacy, section 230's immunity clause protects these sites.[185]

Recently, however, courts have made an effort to narrow the statutory interpretation of section 230[186] and are questioning whether a full liability shield is necessary.[187] In cases where an ISP solicits or edits information, courts are looking to whether ISPs can be held liable for collecting particular types of information.[188] For example, in *Fair Housing Council of San Fernando Valley*

---

[182] *Id.* (citations omitted). *See* Stratton Oakmont, Inc. v. Prodigy Serv. Co., 1995 WL 323710, at *4–5 (N.Y. Sup. Ct. May 24, 1995) (holding that an online computer service could be treated as a "publisher" and therefore be responsible for allegedly libelous statements made by an anonymous poster, even if the server was not aware of the statements).

[183] SOLOVE, *supra* note 30, at 159.

[184] *Id. See*, *e.g.*, Juicy Campus, http://www.juicycampus.com (Last visited Sept. 8, 2008) ("C'mon. Give us the juice. Posts are totally, 100% anonymous.").

[185] SOLOVE, *supra* note 30, at 159 ("These websites thrive under Section 230's broad immunity.").

[186] *See* Chicago Lawyers' Comm. For Civil Rights Under the Law, Inc., v. Craigslist, Inc., 461 F. Supp. 2d 681, 693 (N.D. Ill. 2006) (questioning in dicta the scope of *Zeran* and whether the Craigslist website is a publisher), *aff'd*, 519 F.3d 666 (7th Cir. 2008); *see also* Fair Hous. Council of San Fernando Valley v. Roommates.com, LLC, 489 F.3d 921, 926 (9th Cir. 2007) (holding that creation and development of a discriminatory online questionnaire by the website Roommates.com made it an information content provider with no immunity under section 230).

[187] *See Fair Hous. Council*, 489 F.3d at 927.

[188] *See id.* ("We now turn to the more difficult question of whether the CDA exempts Roommate from liability for publishing and distributing its members' profiles, which it generates from their answers to the form questionnaires.").

v. Roommates.com, LLC, the United States Court of Appeals for the Ninth Circuit found Roomates.com liable with no immunity under section 230 because it created and developed a questionnaire that was discriminatory in nature.[189] The court distinguished its holding from another case, *Carafano v. Metrosplash.com, Inc.*,[190] stating

> *Carafano* provided CDA immunity for information posted by a third party that was not, in any sense, created or developed by the website operator—indeed, that was provided *despite* the website's rules and policies. We are not convinced that *Carafano* would control in a situation where defamatory, private or otherwise tortuous or unlawful information was provided by users in direct response to questions and prompts from the operator of the website.[191]

Another court chose not to follow the standard set by *Zeran* and stated that it was overbroad and inconsistent.[192] In the United States District Court for the Northern District of Illinois decision *Chicago Lawyers' Commission For Civil Rights Under the Law, Inc. v. Craigslist, Inc.*, the court chose instead to look to the plain meaning of section 230. The court found that although the language of the statute does not grant ISP immunity per se, the statute does "prohibit treatment as a publisher, which, quite plainly, would bar any cause of action that requires, to establish liability, a finding that an [ISP] published third-party content."[193] Essentially, the court strived for a more narrow reading of section 230 and observed that it seemed unlikely that Congress had intended to grant broad immunity to ISPs under the CDA that do not screen any third-party content.[194] At a minimum, the court found that section 230(c)(1) bars claims that

---

189 *Id.* at 926–27.

190 Carafano v. Metrosplash.com, Inc., 339 F.3d 1119 (9th Cir. 2007). Metrosplash.com owned a dating Web site that used a questionnaire that a user could fill out to create an online profile. *Id.* at 1120. One of its users created a fake profile using the real information of an actress, Christianne Carafano. *Id.* The information included her home address, phone number, and made lewd remarks about what she liked to do sexually. *Id.* at 1121. The profile attracted attention and the actress received threats and was defamed online. *Id.* at 1121–22. The court did not find Metrosplash.com liable for the actions of the third party, despite the fact that it created the questionnaire used. *Id.* at 1125. The court reasoned that Metrosplash.com did not play an important role in creating, developing, or transforming the information. *Id.*

191 *Fair Hous. Council*, 489 F.3d at 928 (citation omitted).

192 *See Chicago Lawyers' Comm.*, 461 F. Supp. 2d at 695. The court found *Zeran* to be unpersuasive because it "overstate[d] the plain language of Section 230(c)(1)." *Id.* at 693. The court stated that because section 230(c)(1) does not mention the term "immunity" or any similar phrase therein, the interpretation of the law is too broad. *Id.* at 693–94. The court also found *Zeran* inconsistent in its application of immunity to ISPs. It stated that *Zeran* distinguished between ISPs that act like professional publishers versus ISPs that act like a "publisher" by "making information generally known or by disseminating information to the public." *Id.* at 694. In other words, *Zeran* failed to include ISPs that do not edit or choose what information to post, but nevertheless serve as a board for third party postings. *Id.*

193 *Id.* at 696.

194 *Id.* at 697.

require publishing as a critical element with which to find an ISP liable for defamatory comments posted by third parties.[195] The court stated that under their narrow interpretation of section 230, states may enact rules that "induce or require online service providers to protect the interests of third parties . . . ."[196]

The *Roommates.com* and *Craigslist* decisions provide little help to a victim of cyberharassment. Harassment is an act performed by a third party, and under these decisions, ISPs maintain immunity from liability for the unfavorable actions of third parties using their services. The Seventh Circuit decision provided some hope for the cyberharassment victim by reading section 230 in a strict and narrow manner. However, limited legal options exist for cyberharassment victims under section 230, unless a victim can show that a third party's defamatory comments directly responded to the publications by an ISP, or that the ISP participated in or facilitated the defamation.[197]

C. 2001 Report to Congress on Stalking and Domestic Violence

As the new millennium approached, the Federal Government recognized that despite the tremendous benefits the Internet provides,[198] many of its traits—like low cost, ease of use, and anonymous nature—made it an attractive platform for cyberharassers.[199] In 1999, the Department of Justice ("DOJ") released a report, the *1999 Report on Cyberstalking: A New Challenge for Law Enforcement and Industry* ("1999 DOJ Report").[200] The DOJ expanded its findings in 2001 and submitted an additional report to Congress, the *Stalking and Domestic Violence Report to Congress* ("2001 DOJ Report").[201]

---

195 *Id.*

196 *Id.* Under *Zeran*, states would not be able to enact such laws because they would be inconsistent with section 230. *Id.* The holding was affirmed by the U.S. Court of Appeals for the Seventh Circuit in March 2008. Chicago Lawyers' Comm. For Civil Rights Under the Law, Inc., v. Craigslist, Inc., 519 F.3d 666, 671 (7th Cir. 2008).

197 For example, an ISP may solicit defamatory information about individuals as the discriminatory questionnaire at issue in the *Roomates.com* case did. *See* Fair Hous. Council of San Fernando Valley v. Roommates.com, LLC, 489 F.3d 921, 926 (9th Cir. 2007).

198 *See* 1999 DOJ REPORT, *supra* note 26. ("The Internet and other telecommunications technologies are promoting advances in virtually every aspect of society and every corner of the globe: fostering commerce, improving education and health care, promoting participatory democracy in the United States and abroad, and facilitating communications among family and friends . . . .").

199 *Id.*

200 *See id.*

201 U.S. DEP'T OF JUSTICE, STALKING AND DOMESTIC VIOLENCE REPORT TO CONGRESS (2001) [hereinafter 2001 DOJ REPORT], *available at* http:www.ncjrs.gov/pdffiles1/OJP/186157.pdf. The government's use of the term cyberstalking in the 2001 Report is synonymous with the term cyberharassment; thus, what is described as cyberstalking in the report will be referred to as cyberharassment. *See id.* at 1; discussion *supra* Part II.

In the 2001 DOJ Report, the U.S. Attorney General recommended ways to protect people from cyberharassment, including self-help by potential victims, training law enforcement and the Internet industry on the dangers of cyberharassment, and explaining the legal tools available to address the problem.[202] The report highlighted a number of differences between offline and online harassment including differences in proximity between the harasser and the victim.[203] It emphasized that while there are similarities between online and offline harassment, the Internet and other communications mediums such as wireless handheld devices and fax machines provide new methods for harassers to pursue their victims:

> A cyber[harasser] may send repeated, threatening, or harassing messages by the simple push of a button; more sophisticated cyber[harassers] use programs to send messages at regular or random intervals without being physically present at the computer terminal . . . . In addition, a cyber[harasser] can dupe other Internet users into harassing or threatening a victim by . . . [utilizing Internet] bulletin boards or chat room[s] . . . .[204]

The DOJ recommended that states review their existing statutes to determine if they address cyberharassment; if they do not, states should expand their statutes.[205] The report also recommended amending federal law to make it easier to track down cyberharassers while preserving privacy safeguards.[206]

1. Law Enforcement Efforts

The 2001 DOJ Report recognized that for a number of reasons law enforcement has insufficiently responded to cyberharassment, despite the fact that many agencies have large cyberharassment caseloads.[207] Lack of training and expertise of law enforcement officials can frustrate victims and limit law enforcement response.[208] Many cyberharassment crimes go unreported because victims believe the conduct is not grave enough to report or that authorities will not take them seriously.[209] Additionally, law enforcement agencies rarely

---

202 *See* 2001 DOJ REPORT, *supra* note 201, at 12, 14.

203 *Id.* at 3. ("Offline stalking generally requires the perpetrator and the victim to be located in the same geographic area; cyberstalkers may be located across the street or across the country.").

204 *Id.* at 2.

205 *Id.* at 12.

206 *See id.* Specifically, the report stated that amending the CCPA to provide access to subscriber records under the same standards as for e-mail subscribers would make it more feasible to track down cyberharassers and keep privacy safeguards intact. *Id.*

207 *See id.* at 5 ("Based on recent informal surveys of law enforcement agencies, it appears that the majority of law enforcement agencies have not investigated or prosecuted cyberstalking cases.").

208 *See id.*

209 *Id.*

have the appropriate training to recognize a cyberharassment crime and investigate the offense.[210] Such inadequacies result in cyberharassment victims being told by police and law enforcement to either turn off their computers or come back online when a cyberharasser goes offline.[211]

The 2001 DOJ Report also recognized the jurisdictional limitations involved and the frustrations that arise when agencies attempt to investigate a cyberharassment crime across state lines.[212] It acknowledged that there is a lack of consistent statutory authority—some state laws explicitly punish violators for harassment over electronic mediums, while others punish online harassment by amending existing, traditional anti-harassment statutes.[213] Furthermore, in states that do not specify cyberharassment in any statutory form, cyberharassment may not be considered a crime.[214]

In addition, the 2001 DOJ Report recognized that federal law can limit an agency from investigating a harasser in cyberspace.[215] Specifically, the Cable Communications Policy Act of 1984 ("CCPA") bans "disclosure of cable subscriber records without a court order and advance notice to the subscriber."[216] This is significant because a large percentage of Americans subscribe to broadband Internet access through their cable providers.[217] Therefore, the CCPA imposes a considerable hurdle that law enforcement agencies must overcome to investigate cybercrimes like cyberharassment.[218] To alleviate the problem, the 2001 DOJ Report suggested harmonizing federal law by providing agencies access to cable subscriber records under the same privacy protections that govern law enforcement access to e-mail subscribers.[219]

---

[210] 2001 DOJ REPORT, *supra* note 201, at 5.

[211] *See id.* at 5, 8 ("Responding to a victim's complaint by saying 'turn off your computer' or 'change your telephone number' is not acceptable.").

[212] *See id.* at 12. For further discussion on jurisdictional limitations, see *infra* Part V.A.

[213] 2001 DOJ REPORT, *supra* note 201, at 6; *see infra* Part V.A.

[214] 2001 DOJ REPORT, *supra* note 201, at 6.

[215] *Id.*

[216] *Id. See* 47 U.S.C. § 551(c), (h) (2000).

[217] *See* FCC, TRENDS IN TELEPHONE SERVICE 2-3 tbl.2.1 (2008), *available at* http://hraunfoss.fcc.gov/edocs_public/attachmatch/DOC-284932A1.pdf (based on the number of lines, not necessarily the number of subscribers). In June 2007, there were approximately 34.4 million cable modem lines and approximately 29 million ADSL and fiber lines. *Id.*

[218] *See* 2001 DOJ REPORT, *supra* note 201, at 6.

[219] *Id.*; *see also* 18 U.S.C. § 2703 (2006). The relevant portion of the statute states

> (2) A provider of electronic communication service or remote computing service shall disclose to a governmental entity the—
>
> (A) name; (B) address; (C) local and long distance telephone connection records, or records of session times and durations; (D) length of service (including start date) and types of service utilized; (E) telephone or instrument number or other subscriber number or identity, including any temporarily assigned network address; and (F) means and source of payment for such service (including any credit card or bank account number), of a subscriber to or customer of such service when the governmen-

The 2001 DOJ Report further recognized that anonymity is a very serious complication in investigating and prosecuting cyberharassment crimes.[220] As evidenced by cases like *Zeran*, the Internet makes sending anonymous communications relatively simple.[221] This makes it difficult for victims, ISPs, and law enforcement to find and identify the individual or group responsible for defamatory or harassing communications.[222] A possible solution to this problem is tracing electronic communications, but it would require a significant modification of law enforcement methods for surveillance and investigation.[223] In addition, proper training for law enforcement officials that would make them technologically proficient would allow for the efficient enforcement of cybercrimes.[224]

2. Industry Efforts

The 2001 DOJ Report also established that despite an attempt by the Internet industry to inhibit abusive electronic communications, it has not addressed cyberharassment in particular.[225] Instead, ISPs focused on providing consumers with techniques to avoid online harassment rather than establishing anti-harassment programs.[226] The 2001 DOJ Report listed a number of obstacles that cyberharassment victims must overcome to receive help from their ISPs, such as hard-to-find complaint procedures, vague policies on what constitutes harassment, and lack of follow-up on complaints.[227] ISPs responded that although providing such protection is in the best interest of their customers, imposing additional reporting and response requirements on ISPs is very costly

---

tal entity uses an administrative subpoena authorized by a Federal or State statute or a Federal or State grand jury or trial subpoena or any means available under paragraph (1).

[220] 2001 DOJ REPORT, *supra* note 201, at 6 (noting also that anonymity provide the harasser with an advantage over the victim and law enforcement).

[221] *See* 1999 DOJ REPORT, *supra* note 26; 2001 DOJ REPORT, *supra* note 201, at 6–7. Anonymous e-mail communications include two forms:

> The first [form] allows individuals to create a free electronic mailbox through a web site. . . . [S]uch services almost never authenticate or otherwise confirm this information. . . . The second form comprises mail servers that purposefully strip identifying information and transport headers from electronic mail. By forwarding [e-mail] through several of these services serially, a stalker can nearly perfectly anonymize the message.

1999 DOJ REPORT, *supra* note 26.

[222] 2001 DOJ REPORT, *supra* note 201, at 7.

[223] *See id.* ("Traditional law enforcement techniques for surveillance, investigation, and evidence gathering require modification for use on computer networks and often require the use of unfamiliar legal processes.").

[224] *Id.* at 8.

[225] *Id.*

[226] *Id.*

[227] *Id.*

and could result in smaller ISPs losing capital, thereby placing them at a competitive disadvantage.[228]

The 2001 DOJ Report stated that the Internet industry, however, made a considerable effort to inform consumers on methods to protect themselves online.[229] Various programs have been implemented, such as the Cybercitizen Partnership of 1999 ("Partnership"). The Partnership is an agreement between the Internet industry and the Federal Government, focusing on raising public awareness of computer crime issues, specifically those that target children and adolescents.[230] Other initiatives focus on enabling consumers to protect themselves from unsolicited communications.[231] Overall, the Internet industry believed that the best way to address the cyberharassment problem was by educating consumers.[232] Moreover, the 2001 DOJ Report recognized that closer cooperation between the Internet industry and law enforcement would better serve consumers in combating cyberharassment.[233]

V. EXISTING POLICY ADDRESSING CYBERHARASSMENT AND A PROPOSED FEDERAL STATUTORY SCHEME

A. State Legislation

Law enforcement agencies estimate that 20% to 40% of all stalking cases involve electronic means.[234] Currently, forty-five states have enacted laws that explicitly qualify certain types of electronic forms of communication as cyberharassment.[235] Some states include cyberharassment as part of their general harassment statutes. The language of general harassment statutes can, but does not always, include specific references to electronic communications as a

---

[228] *Id.* Furthermore, the Internet industry asserted that the decentralized nature of the Internet makes it difficult for ISPs to collect and submit report on data for undefined issues like cyberharassment. *Id.*

[229] *Id.* at 9. Various initiatives have been implemented to assist consumers in protecting themselves, such as Project OPEN (Online Public Education Network) and GetNetWise.com. *Id.*; Get Net Wise, http://www.getnetwise.org.

[230] 2001 DOJ REPORT, *supra* note 201, at 9. The DOJ and the Information Technology Association of America created the Partnership. *Id.* In addition to boosting public awareness, the Partnership also sought to "provide resources for government to draw on in addressing computer crime." *Id.*

[231] *Id.* For example, when consumers are in Internet chat rooms, they have the ability to block or ignore messages from those who are attempting to harass them. Users also have devices on their e-mail accounts that block cyberharassers. *Id.*

[232] *Id.*

[233] *See id.* at 10.

[234] National Conference of State Legislatures, State Computer Harassment or "Cyberstalking" Laws, Dec. 19, 2007, http://www.ncsl.org/programs/lis/cip/stalk99.htm.

[235] *See id.*

source of harassment.[236] Other states have enacted entirely separate laws for cyberharassment.[237] For example, Florida includes cyberharassment as part of its general harassment law,[238] whereas North Carolina has a separate section for cyberharassment under its computer crime statutes.[239]

More often than not, however, the "current patchwork" of active state cyberharassment laws limits the protection of victims. Sometimes state harassment laws neglect victims altogether because "conflicting state statutes—riddled with complex jurisdictional issues—often deter law enforcement from ever getting involved."[240] For instance, in Missouri, cyberharassment currently qualifies as a misdemeanor,[241] whereas in Illinois, it is considered a class 4 felony.[242] Furthermore, the requisite intent to cause emotional distress in a victim may also differ across states. The penalties for cyberharassment can also vary.[243] Because no federal law addressing cyberharassment exists, the prob-

---

[236] *See* Valetk, *supra* note 18; *see also* National Conference of State Legislatures, *supra* note 234 ("State laws that do not include specific references to electronic communication may still apply to those who threaten or harass others online, but specific language can make the laws easier to enforce.").

[237] *See* Valetk, *supra* note 18.

[238] *See In re* Standard Jury Instructions in Criminal Cases, 953 So. 2d 495, 496 (Fla. 2007) ("To prove the crime of Stalking, the State must prove the following element beyond a reasonable doubt: (Defendant) willfully, maliciously, and repeatedly [followed] ~~or~~ [harassed] or [cyberstalked] (victim)." (alternations and parentheses in original)).

[239] *See* N.C. GEN. STAT. § 14-196.3 (2005). The relevant portion of the statute states

> (b) It is unlawful for a person to:
>
> (1) Use in electronic mail or electronic communication any words or language threatening to inflict bodily harm to any person or to that 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.
>
> (2) Electronically mail or electronically communicate to another repeatedly, whether or not conversation ensues, for the purpose of abusing, annoying, threatening, terrifying, harassing, or embarrassing 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 abuse, annoy, threaten, terrify, harass, or embarrass.
>
> (4) Knowingly permit an electronic communication device under the person's control to be used for any purpose prohibited by this section.

Id.

[240] Valetk, *supra* note 18; *see* 1999 DOJ REPORT, *supra* note 26 ("Some state and local law enforcement agencies also have been frustrated by jurisdictional limitations.").

[241] *See* MO. REV. STAT. § 565.225(4) (Supp. 2007) ("The crime of stalking [offline or through electronic communications] shall be a class A misdemeanor for the first offense.). The statute may soon be amended to implement federal penalties for cyberharassment. *See* Megan Meier Cyberbullying Prevention Act, H.R. 6123, 110th Cong. (2008).

[242] *See* 720 ILL. COMP. STAT. § 5/12-7.5(c) (2006) ("Cyberstalking is a Class 4 felony. A second or subsequent conviction for cyberstalking is a Class 3 felony.").

[243] *Compare* MASS. GEN. LAWS ANN. ch. 265 § 43(a) (West 2008) (making a threat with

lems of inconsistent statutes persist, and the need for a uniform federal statute becomes evident.

B. Video Voyeurism Statutes

As the need for effective cyberharassment laws becomes more apparent, Congress is taking notice and starting to address various types of interactive harassment. Congress has recognized different degrees of privacy that advance protection beyond the traditional idea that when in public, people have no legitimate expectations of privacy.[244] One illustration of this recognition is legislation against video voyeurism, the video version of "gratification derived from [secretly] observing the genitals or sexual acts of others."[245] Technological convergence and advances in digital photography have made video voyeurism relatively easy.[246] For instance, cell phones with still photo or video capture capabilities allow a perpetrator to take nude pictures or "upskirt" photos (those taken up women's skirts) and quickly post them online.[247] Video voyeurism can rise to the level of stalking when stalkers use new technology to monitor their victim's movements.[248] A stalker could monitor a victim's movements, for example, by implanting micro cameras to observe and monitor the victim in her home.[249]

Similar to the problems presented by differing state cyberharassment laws, states address video voyeurism in different and sometimes conflicting ways.[250] Some have separate video voyeurism laws and others have added the proper language to existing statutes.[251] Accordingly, courts are approaching and interpreting the concept of privacy differently in the context of reviewing video voyeurism laws.

---

the intent to place a person in imminent fear a crime of stalking), *with* VA. CODE ANN. § 18.2-60(A)(1) (2004) (making any person who knowingly communicates in a writing, which includes an electronically transmitted writing, threats to harm that person or his family guilty of a class 6 felony).

244 SOLOVE, *supra* note 30, at 166 (discussing the need to rethink the "binary" notion of public privacy in public).

245 BLACK'S LAW DICTIONARY 1609 (8th ed. 2004).

246 SOLOVE, *supra* note 30, at 166.

247 *Id.*

248 *New Frontiers of Stalking—Video Voyeurism*, STALKING RES. CTR. NEWSLETTER (Stalking Res. Ctr., Wash., D.C.), Winter 2003, at 1–2, *available at* http://www.ncvc.org/src/AGP.Net/Components/DocumentViewer/Download.aspxnz?DocumentID=33502.

249 *Id.* ("While the activities of stalking and video voyeurism seem related, it is still unclear as to what the exact relationship is between them. . . . What is not clear . . . is whether the use of this technology alone can be considered a form of stalking.").

250 *Id.*

251 *Id. Compare* CAL. PENAL CODE § 647(a) (West 2002) (lewd conduct in public), *with* S.C. CODE ANN. § 16-3-1700 (2001) (harassment and stalking).

In one case, two men took upskirt photos of unsuspecting women in a mall.[252] Both men were caught and were convicted under a video voyeurism statute in Washington State.[253] The Washington Supreme Court later overturned the conviction because the "plain language of the statute" did not cover an intrusion of privacy in a public place.[254] The court stated that "casual surveillance frequently occurs in public. Therefore, public places could not logically constitute locations where a person could reasonably expect to be safe from casual or hostile intrusion or surveillance."[255] However, the Washington legislature disagreed that taking upskirt photos was a form of casual surveillance and later amended the applicable statute to cover surveillance in both public and private places.[256]

Other states extended protection to different locations where a person *can* reasonably expect to have privacy. For example, the Supreme Court of New Jersey overturned a lower court decision and found a husband's video surveillance of his estranged wife as both harassment and stalking.[257] The court reasoned that under the totality of the circumstances, the husband's conduct could constitute harassment and stalking rather than one or the other.[258]

At the federal level, in an effort to clarify when video voyeurism qualifies as a crime, Congress enacted the Video Voyeurism Prevention Act in 2004.[259] It criminalized video voyeurism and explicitly stated that the act is unlawful, regardless of whether it is committed in public or private areas.[260] The statute, however, only applies to video voyeurism committed on federal property,

---

[252] State v. Glas, 54 P.3d 147, 149 (Wash. 2002).

[253] *Id.* The relevant portion of the statute states

> (2) A person commits the crime of voyeurism if, for the purpose of arousing or gratifying the sexual desire of any person, he or she knowingly views, photographs, or films another person without that person's knowledge and consent while the person being viewed, photographed, or filmed is in a place where he or she would have a reasonable expectation of privacy

REV. CODE WASH. § 9A.44.115 (West 2003).

[254] *Glas*, 54 P.3d at 151.

[255] *Id.* at 150.

[256] H.B. 1001, 58th Leg., Reg. Sess. (Wash. 2003) (enacted); REV. CODE WASH. § 9A.44.115 (West 2003).

[257] H.E.S. v. J.C.S. 815 A.2d 405, 408 (N.J. 2003).

[258] *Id.* at 415 (quoting Cesare v. Cesare, 713 A.2d 390, 395 (N.J. 1998) ("[C]ourts must consider the totality of the circumstances to determine whether the harassment statute has been violated.")).

[259] Pub. L. No. 108-495, 118 Stat. 3999 (2004) (codified as amended at 18 U.S.C. § 1801) ("Whoever . . . has the intent to capture an image of a private area of an individual without their consent, and knowingly does so under circumstances in which the individual has a reasonable expectation of privacy, shall be fined under this title or imprisoned not more than one year, or both.").

[260] 18 U.S.C. § 1801 (2006).

which excludes most local shopping centers.[261] Accordingly, video voyeurism, when committed in *all* public and private places is still not a criminal act under federal law, and thus, states are forced to craft and enforce laws governing public and private places.[262] This further illustrates the need for a uniform federal statute that provides a person with a reasonable expectation of privacy in public places and criminalizes video voyeurism and other types of cyberharassment.

C. Interstate Communications

Section 875(c) of Title 18 of the U.S. Code makes it a federal crime to transmit communication via interstate commerce—including through telephone, e-mail, beepers, and the Internet—that contains a threat to injure another person.[263] Violators may spend up to five years in prison and face significant fines.[264] Although 18 U.S.C. § 875(c) is an important anti-harassment statute, its application to cyberharassment is limited. First, the statute applies to actual threats and does not reach cases where a violator engages in cyberharassment that is meant to annoy or cause emotional distress.[265] Also, the statute may or may not apply to situations where an initial harasser encourages third parties to harass a certain person.[266]

D. Violence Against Women and Department of Justice Reauthorization Act of 2005

In 2005, the Violence Against Women and Department of Justice Reauthorization Act ("Violence Against Women Act") was enacted as an amendment to 47 U.S.C. § 223.[267] The original statute prohibited anyone from using a

---

[261] *See* SOLOVE, *supra* note 30, at 167.

[262] *See id.*

[263] 18 U.S.C. § 875(c) (2006).

[264] *Id; see* United States v. Alkhabaz, 104 F.3d 1492, 1501 (6th Cir. 1997) (Krupansky, J., dissenting)

> The words in section 875 are simple, clear, concise, and unambiguous. The plain, expressed statutory language commands only that the alleged communication must contain *any threat* to kidnap or physically injure *any person*, made for *any reason* or no reason. Section 875(c) by its terms does *not* confine the scope of criminalized communications to those directed to identified individuals . . . .

Id.

[265] 2001 DOJ REPORT, *supra* note 201, at 10 ("[Section 875] applies to communications of actual threats and cannot be used in a case where a stalker engaged in a pattern of conduct intended to harass or annoy another.").

[266] *Id.* at 12.

[267] Violence Against Women and Department of Justice Reauthorization Act of 2005, Pub. L. No. 109-162, 119 Stat. 2960, 2987 (2006); 47 U.S.C. § 223 (2000).

telephone or electronic device "without disclosing his identity and with intent to annoy, abuse, threaten, or harass any person . . . ."[268] Section 113 of the Violence Against Women Act broadened the statute to apply to "any device or software that can be used to originate telecommunications or other types of communications that are transmitted, in whole or in part, by the Internet."[269]

The amendment caused great backlash from First Amendment scholars and those pushing to criminalize cyberharassment.[270] Primarily, First Amendment issues arise because the provision is worded so broadly that it could chill annoying Web speech meant to inform.[271] Unlike the one-to-one communication of telephone calls, the Internet is a forum for public speech. Because of its public nature, speech on the Internet garners more First Amendment protections.[272] Section 113 of the Violence Against Women Act therefore is subject to higher constitutional scrutiny because it applies to the Internet. Furthermore, the amendment threatens to criminalize the very act of communicating anonymously, a right the First Amendment protects.[273]

Second, a fundamental part of the statute is the mens rea provision: a person must have the "intent to annoy, abuse, threaten, or harass any person."[274] The statute likely will prove successful when applied narrowly to individuals who intend to harass a person.[275] However, as evidenced in cases like that of Megan Meier, intent to harass a person often cannot be proven. Moreover, if the statute omits the intent requirement, it becomes far too broad to be effective.

Third, section 223 applies only to direct communications between the harasser and his victim.[276] Therefore, unless the anonymous harasser can be traced, the Violence Against Women Act would not apply to a cyberharassment situation if the harassment occurs over an ISP bulletin board or chat room. Finally, violation of section 223 results only in a misdemeanor punishable by no more than two years in prison rather than a felony with a harsher and longer penalty.[277]

---

268 47 U.S.C. § 223(a) (2000).

269 Violence Against Women and Department of Justice Reauthorization Act § 113.

270 *See* Wendy McElroy, *Does New Cyberstalking Law Criminalize Free Expression?*, FOXNEWS.COM, Jan. 17, 2006, http://www.foxnews.com/story/0,2933,181958,00.html.

271 *Id.*

272 *Id.*

273 Posting of Kurt Opsahl, *Here We Go Again: Law Attempts to Limit Anonymous Online Speech*, to Electronic Frontier Foundation Deeplinks Blog, http://www.eff.org./deeplinks/2006/01/here-we-go-again-law-attempts-limit-anonymous-online-speech (Jan. 9, 2006). *See* discussion *supra* Part II.B; *see also* Talley v. California, 362 U.S. 60, 65 (1960) ("[A]nonymity has sometimes been assumed for the most constructive purposes.").

274 47 U.S.C. § 223(a)(1) (2000).

275 *See* Opsahl, *supra* note 273.

276 2001 DOJ REPORT, *supra* note 201, at 11; 47 U.S.C. § 223 (2000).

277 2001 DOJ REPORT, *supra* note 201, at 11.

E. Legal Solutions: Striking a Balance Between Privacy and Free Speech

The right to free speech is fundamental to a person's "moral and intellectual development," but with it comes the responsibility to ensure that contemporaneous rights, like the right to privacy, are not invaded.[278] The right of individual expression undoubtedly is important. However, mounting evidence suggests that assurance of the right to freedom of expression on the Internet is often at the expense of individual privacy.[279] Due to the lack of government regulation of the Internet and "the historical development of the Internet along laissez-faire principles," a very broad reading of free speech has resulted.[280] In turn, the lenient interpretation of freedom of expression has caused a threat to public safety, as illustrated by cyberharassment. Additionally, issues arise with legislation because of freedom of speech and invasion of privacy challenges.[281]

The problem with most legislation regulating the Internet is that it is too sweeping in nature by proposing to regulate legitimate Web sites and speech in order to punish a small number of violators.[282] For example, the Deleting Online Predators Act, introduced in 2006 by then Rep. Michael Fitzpatrick (R-PA), would "require schools and libraries that receive federal universal service support to block minors' access to social networking sites."[283] Sponsors of the legislation argue that social networking sites like MySpace attract online predators and child pornography.[284] However, as Adam Thierer of the Progress & Freedom Foundation notes, "censoring these sites will do little to weed out these problems and instead merely block access to sites that are socially beneficial."[285]

The solution to combating cyberharassment lies in crafting a narrow federal

---

278 Julie Dare, *Cyberharassment and Online Defamation: A Default Form of Regulations?*, 11 TRANSFORMATIONS (2005), http://www.transformationsjournal.org/journal/issue_11/article04.shtml.

279 *Id.* ("[O]n the Internet, the focus is on the right to freedom of expression, rather than on the responsibility to ensure that this right is exercised with due care and respect for the rights of others.").

280 *Id.* (describing the liberal interpretation of free speech rights on the Internet).

281 Koloff, *supra* note 106 (describing the efforts of the American Civil Liberties Union and other in opposition to cyberbullying laws).

282 ADAM THIERER, PROGRESS & FREEDOM FOUND., IS MYSPACE THE GOVERNMENT'S SPACE?, PROGRESS SNAPSHOT 2.16 at 2 (2006), *available at* http:// www.pff.org/issues-pubs/ps/2006/ps_2.16_myspace.pdf. Because online harassment can involve a "breadth of conduct," anti-cyberharassment statutes usually need to be broad in order to be effective. Simultaneously, because cyberharassment deals with "expressive conduct and speech," anti-cyberharassment statutes have to be formulated and enforced in a way that does not violate speech protected by the First Amendment. 1999 DOJ REPORT, *supra* note 26.

283 THIERER, *supra* note 282, at 1; Deleting Online Predators Act of 2006, H.R. 5319, 109th Cong. § 3 (2006).

284 THIERER, *supra* note 282, at 1.

285 *Id.*

law that prohibits cyberharassment. Any such legislation should aim to meet three criteria. First, cyberharassment should be recognized as harassment towards a person that induces emotional distress or fear of bodily injury over an electronic medium. Second, privacy safeguards should be maintained, meaning that information that is considered private by reasonable individuals should remain private. And third, the right to free speech—the right of a person to express his ideas, so long as they do not aim to inflict fear in a person—should be upheld. This comment proposes the following legislation:

Cyberharassment defined

> Under Congress's Article I commerce power,[286] it shall be unlawful for any person or group, known or anonymous, to utilize a computer network form of electronic communication to target a specific person for no defined purpose, and through the use of words or language, aim to harass, annoy, embarrass, abuse, threaten, induce fear of bodily harm, or a combination thereof, in a victim.
>
> It shall be lawful to trace the Internet Protocol address or equivalent of an anonymous third party utilizing an Internet Service Provider for means of investigating cyberharassment.
>
> It is a misdemeanor, punishable by a fine of up to $500,000, when severe emotional distress inflicted in a victim is a direct result of the above described cyberharassment.
>
> It is a Federal Crime, punishable by up to 10 years in prison, when death of a victim is a direct result of the above described cyberharassment.

This proposed statute is not the exclusive means through which the Federal Government could combat cyberharassment. Rather, it illustrates how cyberharassment can be outlawed without violating privacy or free speech laws. Until the Federal Government enacts an anti-cyberharassment law, the best means with which to combat the issue is to educate consumers.[287] Internet users need to be aware of the consequences of posting personal information online and as a result, the dangers of cyberharassment by individuals and groups.[288] Furthermore, self-help solutions are available. Ignoring communications from those who a person believes to be a potential cyberharasser is the best first step to stop cyberharassment.[289] Traceable anonymity allows victims of cyberharass-

---

[286] U.S. CONST. art. I, § 8, cl. 3 ("To regulate Commerce with foreign Nations, and among the several States . . . .").

[287] *See* National Crime Prevention Council, Delete Cyberbullying, http://www.ncpc.org/newsroom/current-campaigns/cyberbullying (last visited Sept. 3, 2008); WiredSafety.org, http://www.wiredsafety.org/index.html (last visited Sept. 3, 2008).

[288] SOLOVE, *supra* note 30, at 204. A survey of 267 pairs of teens and parents by a psychology professor at California State University-Dominguez Hills reported that two-thirds of parents had never talked with their teens about their MySpace use. Michelle Andrews, *Decoding MySpace*, U.S. NEWS & WORLD REPORT, Sept. 18, 2006, at 50. Additionally, 38% of them had never seen their child's MySpace profile. *Id.*

[289] *See* Aftab, *supra* note 41.

ment to trace their harasser's true identity.[290] Additionally, changing the "architecture" of a Web site will further limit opportunities for cyberharassment.[291] By changing the settings on Web sites to more private defaults, Web site operators ensure better protection of their users from online harassment.[292]

VI. CONCLUSION

As the Internet continues to grow, both public safety concerns and the need for regulations that discourage cyberharassment will become more prominent. The Internet is dynamic. As the Internet evolves and progresses, a failure to adopt cybercrime legislation now will lead to future violations of constitutional rights. What follows is an unbalanced marketplace, where Internet and communications companies are constantly rushing to meet the demand of their consumers by creating new and innovative technologies.[293] But the effect of trying to meet these demands, without regulations in place, further contributes to the threat to public safety and vulnerability of consumers to issues like cyberharassment.

Megan Meier's suicide is one illustration of the tragic consequences that can occur as a result of the unregulated dynamics of the Internet. This Comment, however, does not suggest that the Internet should be regulated. Instead, it calls for recognition by the Federal Government that cyberharassment poses a threat to public safety and that laws prohibiting it are necessary to protect Internet users. Whether and what balance is struck between freedom of speech and the right to privacy will ultimately be determined by the courts. However, the best interest of the public is served by the Federal Government providing a law that addresses both values equally. It is time to enact federal legislation that combats cyberharassment to promote a safe interactive environment for Americans on the Internet.

---

[290] *See* discussion *supra* Part II.B.1. *But see* Tal Z. Zarsky, *Thinking Outside the Box: Considering Transparency, Anonymity, and Pseudonymity as Overall Solutions to the Problems of Information Privacy in the Internet Society*, 58 U. MIAMI L. REV. 991, 1026 (2004) (discussing anonymity as a means for protecting privacy and proposing "one-time identities that cannot be traced back to their actual selves").

[291] For example, a social networking Web site has control over the default privacy settings for its users. On MySpace, the default privacy setting for its users is set so that anybody can view another person's profile. SOLOVE, *supra* note 30, at 200–01.

[292] *Id.* at 201.

[293] Harry A. Valetk, *Mastering the Dark Arts of Cyberspace: A Quest for Sound Internet Safety Policies*, 2004 STAN. TECH. L. REV. 2, ¶ 84 (2004), http://stlr.stanford.edu/STLR/Articles/04_STLR_2/index.htm.