Cyberharassment Is a true Danger: Is the Solution Found in Copyright Law?

by

Izak J. Post

Submitted in partial fulfillment of the requirements of the

King Scholar Program

Michigan State University College of Law

Under the direction of

Professor Barbara O'Brien

Spring, 2013

Contents

I. Introduction

Currently, there are a lot of people in the world that think cyberharassment is not a significant and dangerous threat. Even police and judges often have flippant responses to cyberharassment claims. In a recent cyberharassment case, William Cassidy wrote nearly 8,000 tweets[1] about Alyce Zeoli.[2] Most of the tweets were very threatening.[3] The judge decided that

[1] Tweets are small messages sent from the social media site Twitter.com. Users can send messages to other users. For more information visit http://support.twitter.com/articles/13920-get-to-know-twitter-new-user-faq.
[2] Somini Sengupta, *Case of 8,000 Menacing Posts Tests Limits of Twitter Speech*, N.Y. TIMES (Aug, 26, 2011), http://www.nytimes.com/2011/08/27/technology/man-accused-of-stalking-via-twitter-claims-free-speech.html?_r=0.
[3] Two examples of the tweets are: "Do the world a favor and go kill yourself" and "Ya like haiki? Here's one for ya. Long limb, sharp saw, hard drop." Lauren Dugan, *Is it Cyberstalking To Tweet 8,000 Times Telling Someone To*

Cassidy was protected by the First Amendment. The judge said that Zeoli "had the ability to protect her 'own sensibilities simply by averting' her eyes from the Defendant's Blog and not looking at, or blocking his Tweets."[4] Some people have interpreted the decision as the judge not fully "understanding the technology involved or how common the Internet is in everyone's lives."[5] Police do not understand this new crime either. One woman being harassed on the internet went to the police and they told her to "stay offline."[6] Obviously, someone in this day and age cannot stay offline, and even if the victim can stay offline, their potential employers will not, which will perpetuate the harm to the victim.

To understand why cybercrimes are such a problem, it is important to read about individuals being victimized. Personal accounts of cyberharassment victims makes clear that cyberharassment is a very real problem and demands drastic changes to the law in order to adequately protect its victims. That is why this paper starts with discussing real stories of actual cyberharassment. Unfortunately, some of the language used to harass can be graphic. In recounting the victim's stories, this paper will limit the indecent language to only what is necessary.

One of the main problems with cyberharassment laws is that usually no one is held responsible for the harm caused. The victim cannot sue the actual perpetrator because cyberharassers use anonymous names and software to shield their identity. The victim cannot sue the website because they are immune from liability through section 230 of the Communications

---

"Go Kill Yourself"?, MEDIABISTRO (Aug. 30, 2011), http://www.mediabistro.com/alltwitter/is-it-cyberstalking-to-tweet-8000-times-telling-someone-to-go-kill-yourself_b13236.

[4] United States v. Cassidy, 814 F. Supp. 2d 574, 585 (D. Md. 2011), *appeal dismissed* (Apr. 11, 2012).

[5] Marjorie Korn, *Alissa Blanton's Stalker Only Needed a Computer and a Wi-Fi Connection to Make Her Life a Living Hell*, SELF MAGAZINE, Jan. 2013. at 108 quoting Shanlon Wu, Alyce Zeoli's attorney.

[6] *Id*. at 107.

Decency Act.[7] The website is not even legally bound to remove the offending content from its pages. The second part of this paper discusses how cyberharassment law has developed and explains the shortcomings of the current laws.

In order for cyberharassment victims to experience any kind of relief, the Internet Service Providers (ISP), and website owners must be held liable for any cyberharassment that occurs on their servers or websites.[8] However, determining the appropriate amount of liability is difficult. This is where internet copyright infringement law can help shape new cyberharassment laws. Internet copyright infringement law holds ISPs liable for its subscribers' violations if the ISP did not follow certain steps. The third part of this paper discusses the details of Internet copyright infringement law. Finally, the last section of this paper discusses the similarities between cyber-copyright law and cyberharassment law, and proposes a legislative solution to the shortcomings of current cyberharassment law modeled after the Digital Millennium Copyright Act.[9]

II. Case Study

One form of cyberharassment is On-Line Mobs. According to Daniel Citron[10] online mobs can use four types of attacks in their online assaults. "First, attacks involve threats of physical violence," including death and rape threats.[11] Next, the assaults invade the victim's privacy. The attackers hack into the victim's computer and steal personal information, including a social security number, phone number, and other personal information and then post that

[7] Communications Decency Act, 47 U.S.C. § 230 (2000).
[8] In this paper, the term Internet Service Provider, or ISP, is used very broadly to include any provider of online services or network access.
[9] Digital Millennium Copyright Act, 17 U.S.C. § 512 (2006).
[10] Danielle Citron is a law professor at University of Maryland Francis King Carey School of Law. One of her main areas of research is civil rights. She has published several papers that discuss how cyberharassment affects civil rights. *Faculty*, UNIVERSITY OF MARYLAND FRANCIS KING CAREY SCHOOL OF LAW (May, 6, 2013), http://www.law.umaryland.edu/faculty/profiles/faculty.html?facultynum=028.
[11] Danielle Keats Citron, *Cyber Civil Rights*, 89 B.U. L. Rev. 61, 69 (2009).

information on line.[12] Third, the assaults can damage the victim's reputation and economic opportunities. The attackers will post lies about the victim and send those lies to the victim's employer.[13] Lastly, attackers can use technology to force victims offline by coordinating denial-of service attacks.[14] Often, these online mobs use all four tools to attack.

In 2007, the website AutoAdmit, an online discussion board specifically for prospective and current law students,[15] was home to a whole slew of attacks on female law students. The posters threatened two Yale law students with violence. One poster said that a named student "should be raped."[16] Other posters responded; one poster said, "I'll force myself on [identified student]" and "sodomize" her "repeatedly."[17] Another post said that the student "deserves to be raped so that her little fantasy world can be shattered by real life."[18]

Discussion threads on AutoAdmit suggested the posters had physical access to the two victims. Posts would often include descriptions of what the victims were wearing that day or discussions about following the victims to the gym. Posters also posted pictures of the victims to AutoAdmit.[19] Also, the personal email address of one victim was posted on the website with an encouraging note to email her if you are mad at her.[20] Additionally, posters stated damaging and untrue things about each victim. For instance, posters claimed that the victims had spent time in a drug rehabilitation center, were having a lesbian affair with a law school administrator, posed in

---

[12] *Id*. at 70.
[13] *Id*. at 70-71.
[14] *Id*. at 71. A denial of service attack is when "an attacker attempts to prevent legitimate users from accessing information or services." The most common type of denial of service attack is when an "attacker floods a network with information." *Understanding Denial of Service Attacks*, US-CERT (Feb. 6, 2013), http://www.us-cert.gov/ncas/tips/ST04-015.
[15] *Law School*, AUTOADMIT (May 6, 2013), http://www.xoxohth.com/. AutoAdmit calls itself "the most prestigious law school discussion board in the world." *Id*.
[16] Danielle Keats Citron, *Cyber Civil Rights*, 89 B.U. L. REV. 61, 72 (2009).
[17] *Id*.
[18] *Id*.
[19] *Id*.
[20] *Id*.

playboy, had sexually transmitted diseases, and had sub-par LSAT scores. Again, the two victims said that these statements were lies.[21]

Not only did the posters write malicious lies on AutoAdmit, but they also took action to actively spread lies to the victims' employers and professors. Posters sent emails to the victims' summer employers spreading lies in an attempt to make sure they did not get hired.[22] The posters directly emailed professors with similar intentions.[23] The harassers sent the emails using anonomyzing software so the emails could not be traced back to them.[24] Lastly, posters started a "Google Bombing"[25] campaign to make the results of internet searches of the victim's names the disgusting comments and lies the posters were writing.[26]

Finally, the two victims filed a lawsuit against the posters. The law suit alleged that the victims asked AutoAdmit to take down the offensive threads and the website refused.[27] The site owner, Jarret Cohen, admitted to receiving the requests but said he ignored the request because the victim threatened to sue him.[28] Cohen also said that he dismissed another complaint "because it sounded like more of the kind of juvenile stuff that I have heard going on that people complained about for years."[29] Unfortunately, AutoAdmit is completely immune from liability because of the Communications Decency Act, section 230.[30]

---

[21] *Id*. at 72-73.
[22] *Id*. at 73.
[23] *Id*. at 73.
[24] *Id*. at 73.
[25] A Google bomb is an "attempt to influence the rankings of a given site in results returned by the Google search engine." *Google Bombing*, LINKS & LAW (May 6, 2013), http://www.linksandlaw.com/technicalbackground-google-bombing.htm. Essentially, this is accomplished by using a specific phrase and linking that phrase to a specific person or webpage. *Id*.
[26] Danielle Keats Citron, *Cyber Civil Rights*, 89 B.U. L. Rev. 61, 73 (2009).
[27] *Id*. at 74.
[28] *Id*. at 75 n.87.
[29] *Id*.
[30] Communications Decency Act, 47 U.S.C. § 230 (2000).

The two victims also filed against the 39 anonymous posters.[31] After filing a complaint against anonymous defendants, the victims had to determine the true identity of the posters. The victims tried posting on AutoAdmit demanding that the posters come forward and identify themselves.[32] Not surprisingly, this yielded no names. Next, the victims petitioned ISP for identifying information of the posters. However, this was unsuccessful as well, in part because the harassers had taken steps to eliminate their cyber-footprint.[33] In this case the victims were lucky because several perpetrators came forward. Most of the defendants settled with the victim for money in the four digits.[34] The biggest punishment for some of the offenders is not the civil settlement, but the hardship they now have to endure to pass the character and fitness portion of the State bar application.[35]

This case is an anomaly because it has a happy ending. The victims of the cyberharassment found the harassers and sued them. Despite how successful these two students were in punishing their harassers, they were unsuccessful at removing the disgusting posts that would result from searching their names.[36] When employers would Google their names, titles of posts would appear about rape and STDs.[37] The immediate harm of being harassed and scared was remedied, but the ongoing harm to their internet reputation is ongoing. Unfortunately, the victims have no legal recourse because AutoAdmit, and every other website, has complete

[31] Danielle Keats Citron, *Cyber Civil Rights*, 89 B.U. L. Rev. 61, 73 n.70 (2009).
[32] David Margolick, *Slimed Online*, UPSTART BUSINESS JOURNAL (Aug. 4, 2011), http://upstart.bizjournals.com/news-markets/national-news/portfolio/2009/02/11/Two-Lawyers-Fight-Cyber-Bullying.html?page=all.
[33] *Id*.
[34] *Id*.
[35] *Id*.
[36] Cohen eventually had a change of heart and removed a lot of the more nasty comments on the website. *Id*.
[37] *Id*.

immunity from liability and cannot be forced to remove offensive posts about people.[38] Even in a highly successful cyberharassment case, like this one, the victims are left still feeling the harm their harassers put them through.

III. Background

The tort of defamation and the crime of harassment are similar, especially in the cyber context. Defamation is "the act of harming the reputation of another by making a false statement to a third person."[39] Harassment is using words, conduct, or action to cause a person substantial emotional distress that serves no legitimate purpose.[40] Often times a cyberharasser will defame someone as part of their campaign to harass them, as illustrated above. The laws regarding defamation and its history leading up to the Communications Decency Act have had a substantial effect on current cyberharassment laws.

A. History of Defamation

At common law, liability for defamation included not only the original speaker, but also the "secondary disseminators who subsequently transmitted the harmful information."[41] Originally, secondary disseminators were strictly liable for any harm that resulted from their reproduction or dissemination of the defamatory material.[42] However, the courts have modified this rule and have now classified secondary disseminators into three categories: Publishers, distributors, and common carriers.[43] Each category has a different standard of liability.

---

[38] Communications Decency Act, 47 U.S.C. § 230 (2000); *see also* Zeran v. America Online, Inc., 958 F. Supp. 1124 (E.D. Va. 1997), *aff'd*, 129 F.3d 327 (4th Cir. 1997).
[39] BLACK'S LAW DICTIONARY 479 (9th ed. 2009).
[40] BLACK'S LAW DICTIONARY 784 (9th ed. 2009).
[41] Brian C. McManus, Note, *Rethinking Defamation Liability for Internet Service Providers*, 35 SUFFOLK U. L. REV. 647, 650 (2001).
[42] *Id*.
[43] *Id*. at 651.

Common carriers quickly disseminate large volumes of information that they could neither legally nor practically monitor. Common carriers are not liable for defamation "regardless of whether they recklessly or knowingly" distribute the defamatory material.[44] A court will classify an entity as a common carrier if either a statute restricts its ability to monitor or control the information they transmit, or when the entity cannot practically monitor the transmissions because of the volume of information transmitted.[45] An example of a common carrier is a telephone company.[46]

Distributors include libraries, newspaper stands, and other entities that can exercise some discretion in deciding what materials to carry.[47] "Courts will classify entities as distributors when they are theoretically capable of monitoring and controlling all of the information they disseminate, but lack the resources to monitor the information or insure its veracity."[48] A distributor's liability for defamation is limited to a reckless or actual malice standard. They are only liable when they have actual or constructive knowledge of the defamatory material and fail to take action.[49]

A publisher actively participates in choosing the material it disseminates and edits that material.[50] A publisher has the capacity to make sure all the information it publishes is true. For the most part, a publisher's liability is a negligent standard.[51] Unlike a distributor, the publisher does not have to have knowledge of the defamatory material to be liable. Typically, a publisher

---

[44] *Id*.
[45] Brian C. McManus, Note, *Rethinking Defamation Liability for Internet Service Providers*, 35 SUFFOLK U. L. REV. 647, 651 (2001).
[46] *Id*.
[47] *Id*.
[48] *Id*.
[49] *Id*. at 651-52.
[50] *Id*. at 652.
[51] *Id*. at 653.

must take some steps to insure the material they plan to publish is true.[52] The publisher has the highest level of liability because they exercise the most control over the content they publish.[53]

B. Internet Service Providers and Their Proper Classification

The internet created a new form of disseminating information. Soon the courts were asked to answer the question, what liability do ISPs have for defamation committed by their subscribers. In the beginning, courts were inconsistent with how they classified ISPs.[54] In one of the earlier cases regarding false statements and the internet, *Daniel v. Dow Jones & Co*., an investor sued Dow Jones alleging that Dow Jones's on line news service provided false and misleading information.[55] The court determined that Dow Jones controlled all the information it published, similar to a newspaper, and held that Dow Jones should be held to the publisher standard.[56]

Four years later, the case of *Cubby, Inc. v. CompuServe, Inc*. reconsidered the issue of ISP liability for defamatory statements made on their servers.[57] In *Cubby*, the ISP, CompuServe, hosted a service that allowed subscribers' access to online forums and electronic databases.[58] One of the forums posted defamatory material.[59] CompuServe did not dispute that the material was defamatory, but rather its liability as an ISP. The court looked to the degree of editorial control CompuServe exercised.[60] Because CompuServe did not edit all the information that they

[52] *Id*. at 652-53.
[53] *Id*.
[54] *Id*. at 654-55.
[55] Daniel v. Dow Jones & Co., 520 N.Y.S.2d 334, 335-36 (N.Y. Civ. Ct. 1987).
[56] *Id*. at 337-38.
[57] Cubby, Inc. v. Compuserve, Inc., 776 F. Supp. 135 (S.D.N.Y. 1991).
[58] *Id*. at 137.
[59] *Id*. at 138.
[60] *Id*. at 140.

received, the court compared CompuServe to a library and classified CompuServe as Distributor.[61]

Four years after *Cubby*, the courts considered another ISP defamation liability case, *Stratton Oakmont, Inc. v. Prodigy Services Co*.[62] Prodigy was an ISP that ran a virtual bulletin board.[63] Prodigy also advertised themselves as a family network "that: carefully edited and controlled content, maintained and circulated content guidelines, utilized screening software to automatically edit content, and employed editors known as 'board leaders' who were responsible for monitoring the content of information the network distributed."[64] Stratton sued Prodigy because one of Prodigy's two million subscribers wrote defamatory remarks on the bulletin board.[65] The court determined that because Prodigy tried to exercise editorial control over the bulletin board, they were considered a publisher and subject to the negligence standard.[66]

These three cases are reconcilable. The court took an approach that involved a fact intensive inquiry on how much editorial control the ISP undertook. The problem with this approach is that it left a large amount of uncertainty as to what standard an ISP will be held to for its subscribers' defamatory statements. Also, these cases, and especially *Prodigy*, created an incentive not to monitor subscribers' conduct.[67] Congress recognized these problems and addressed the issue with the Communications Decency Act.

---

[61] *Id*.
[62] Stratton Oakmont v. Prodigy Serv. Co., 1995 N.Y. Misc. LEXIS 229 (N.Y. Sup. Ct. May 25, 1995).
[63] *Id*. at *3.
[64] Brian C. McManus, Note, *Rethinking Defamation Liability for Internet Service Providers*, 35 SUFFOLK U. L. REV. 647, 657 (2001); *see also Prodigy*, 1995 N.Y. Misc. LEXIS at *3-*4.
[65] *Prodigy*, 1995 N.Y. Misc. LEXIS at *3.
[66] *Id*. at *10.
[67] Brian C. McManus, Note, *Rethinking Defamation Liability for Internet Service Providers*, 35 SUFFOLK U. L. REV. 647, 657 (2001).

C. The Communications Decency Act

Congress's enactment of section 230 of the Communications Decency Act (CDA) directly addresses ISP liability for defamation as a publisher.[68] Congress gave several reasons for eliminating publisher liability. One specific purpose of section 230 was to address and overrule *Stratton v. Prodigy*.[69] Congress wanted to overrule *Prodigy* because they felt the case discouraged companies from actively monitoring the content on the ISP or creating technology to screen indecent communications.[70] Congress wanted to encourage such "Good Samaritan" activity.[71] Congress adopted these measures because it wanted to promote the development and progress of the internet.[72] After the passage of section 230, it was clear that section 230 eliminated publisher liability for an ISP. However, it was unclear whether Congress wanted section 230 to apply the rule from *Cubby*, and eliminate all ISP liability for subscribers' defamatory comments, including those classified as distributors.[73] When courts heard this issue, they determined that the CDA removed all liability for ISP for all types of defamatory remarks by its subscribers.[74]

In *Zeran v. America Online, Inc*., the court considered whether CDA section 230 applied to ISPs classified as distributors.[75] In this case, someone posing as Zeran posted an advertisement for t-shirts containing offensive remarks about the Oklahoma City bombing on the internet, hosted by America Online (AOL).[76] Zeran began to receive dozens of threatening phone calls

---

[68] Communications Decency Act, 47 U.S.C. § 230 (2000).
[69] H.R. CONF. REP. NO. 104-458, at 194 (1996) ("one of the specific purposes of [Section 230] is to overrule Stratton-Oakmont v. Prodigy and any other similar decisions"). *Id*.
[70] 141 CONG. REC. 22,045 (1995) (remarks of Rep. Cox).
[71] Communications Decency Act, 47 U.S.C. § 230(c) (2000).
[72] Joel R. Reidenberg et al., *Section 230 of the Communications Decency Act: A Survey of the Legal Literature and Reform Proposals*, CENTER ON LAW AND INFORMATION POLICY, Apr. 25, 2012, at 8.
[73] Brian C. McManus, Note, *Rethinking Defamation Liability for Internet Service Providers*, 35 SUFFOLK U. L. REV. 647, 658 (2001).
[74] Zeran v. America Online, Inc., 958 F. Supp. 1124 (E.D. Va. 1997), *aff'd*, 129 F.3d at 327 (4th Cir. 1997).
[75] 958 F. Supp. 1124.
[76] *Id*. at 1126.

because of the offensive postings by the anonymous user.[77] Zeran contacted AOL and requested that AOL remove the offensive material and AOL refused to do so. Zeran filed suit alleging that AOL was negligent in failing to remove the offensive material, despite being made aware of it.[78] Zeran argued that section 230 of the CDA does not limit liability for ISPs classified as distributors, only publishers.[79] Furthermore, Zeran argued, America Online should be classified as a distributor and that they should be liable under the distributor standard.[80] The court rejected Zeran's argument and said that even though the text of section 230 only limits liability for ISPs classified as publishers, Congress intended for the act to apply to "all forms of online defamation analysis including distribution."[81] Since *Zeran*, few courts have examined whether section 230 applies to ISPs characterized as distributors.[82]

D. Cyberharassment Laws

Most states have acknowledged that cyber-crimes have become a serious threat. Accordingly, almost every state has laws that directly address cyberstalking or cyberharassment.[83] States address this new crime by either creating a brand new law[84] or adapting current stalking and harassment law to include online conduct.[85] There are two main types of online behavior that states have addressed: cyberstalking and cyberharassment.

---

[77] *Zeran*, 129 F.3d at 329 (4th Cir. 1997).
[78] *Id*. at 330.
[79] *Zeran*, 958 F. Supp. 1124, 1129 (E.D. Va. 1997).
[80] *Id*. at 1128.
[81] Brian C. McManus, Note, *Rethinking Defamation Liability for Internet Service Providers*, 35 SUFFOLK U. L. REV. 647, 659 (2001); *see also Zeran*, 958 F. Supp. 1124, 1135.
[82] McManus, 35 SUFFOLK U. L. REV. at 659 (2001).
[83] *State Cyberstalking and Cyberharassment Laws*, NCSL (last visited Nov. 16, 2012), http://www.ncsl.org/issues-research/telecom/cyberstalking-and-cyberharassment-laws.aspx.
[84] *See* ARIZ. REV. STAT. § 13-2916 (LexisNexis 2013); MONT. CODE ANN. § 45-8-213 (2013); N.C. GEN. STAT. § 14-196(b) (2013).
[85] *See* ALASKA STAT. § 13A-11-8 (2013); DEL. CODE ANN. tit. 11 § 1311 (2013); HAW. REV. STAT. § 711-1106 (2013).

Although these three crimes are related, it is important to understand the differences. Although the exact definition differs from state to state, stalking is generally defined as, "a course of conduct directed at a specific person that would cause a reasonable person to feel fear."[86] In comparison, "cyberstalking is the use of the Internet, email or other electronic communications to stalk."[87] Some state laws include an element of either physical proximity or a "credible threat" in the stalking statute.[88] "A 'credible threat' is a threat made with the intent and the apparent ability to carry out that threat so as to cause the person who is the target of the threat to reasonably fear for his or her safety."[89] Having a requirement of physical proximity or credible threat can be problematic in the cyber-stalking context because threats over the internet can easily lack the physical proximity or apparent ability element. A cyberstalker who lives on the other side of the country from his victim does not have the apparent ability to follow through with his threats, and, thus, the victim cannot file stalking charges against her stalker.[90]

Cyberharassment is similar to cyberstalking but does not require a credible threat.[91] Most cyberharassment laws contain three elements. First, the poster must have the intent to harass. Second, the message would cause a reasonable person to feel harassed. Third, the victim must

[86] *Stalking*, VICTIMS OF CRIME (last visited May 6, 2013), http://www.victimsofcrime.org/library/crime-information-and-statistics/stalking.
[87] *State Cyberstalking and Cyberharassment Laws*, NCSL (last visited Nov. 16, 2012), http://www.ncsl.org/issues-research/telecom/cyberstalking-and-cyberharassment-laws.aspx.
[88] Naomi Harlin Goodno, *Cyberstalking, A New Crime: Evaluating the Effectiveness of Current State and Federal Laws*, 72 Mo. L. Rev. 125, 134-35 (2007); *see also* FLA. STAT. § 784.048 (2013); ALA. CODE § 13A-6-90 (LexisNexis 2013).
[89] *Stalking*, VICTIMS OF CRIME (May 6, 2013), http://www.victimsofcrime.org/library/crime-information-and-statistics/stalking; *see also* Naomi Harlin Goodno, *Cyberstalking, A New Crime: Evaluating the Effectiveness of Current State and Federal Laws*, 72 Mo. L. Rev. 125, 136 (2007).
[90] Naomi Harlin Goodno, *Cyberstalking, A New Crime: Evaluating the Effectiveness of Current State and Federal Laws*, 72 Mo. L. Rev. 125, 138 (2007).
[91] *State Cyberstalking and Cyberharassment Laws*, NCSL (Nov. 16, 2012), http://www.ncsl.org/issues-research/telecom/cyberstalking-and-cyberharassment-laws.aspx.

actually feel harassed.[92] Every state's harassment laws are different, but most laws have these or similar elements.[93]

E. Shortcomings of Cyberharassment Laws

The fact that thirty nine states have recognized the importance of directly criminalizing cyberharassment is a large step in the right direction.[94] However, these laws bring enforcement challenges. There are three main cyberharassment law enforcement challenges. The first main challenge is learning the identity of a harasser on the Internet. Some of the harassers are technologically sophisticated and know how to remain anonymous. They often use public computers and anonymizing software to hide their identities when making their illegal, harassing comments. If the victims cannot identify their harassers, then the victims cannot seek any real remedy.

The second challenge is that even if a victim learns the identity of her harasser, the harasser is unlikely to have enough money to adequately compensate the victim. In the AutoAdmit case the victims settled for an amount in the 4 digit range.[95] That is not very high considering how much they suffered.

The third and most important challenge is getting the ISP to remove the offending material once the victim discovers it. What distinguishes cyberharassment from regular harassment is that once the imminent harassment has stopped, there remains a cyber-footprint of everything that was said. Also, everyone with internet access can read the harassing comments.

---

[92] MICH. COMP. LAWS § 750.411s.

[93] *State Cyberstalking and Cyberharassment Laws*, NCSL (Nov. 16, 2012), http://www.ncsl.org/issues-research/telecom/cyberstalking-and-cyberharassment-laws.aspx. Cyberbullying and cyberharassment are sometimes used as synonyms, but cyberbullying generally refers to electronic harassment among minors in a school setting. Essentially, cyberbullying is a subset of cyberharassment. *Id*.

[94] *Id*.

[95] David Margolick, *Slimed Online*, UPSTART BUSINESS JOURNAL (Aug. 4, 2011), http://upstart.bizjournals.com/news-markets/national-news/portfolio/2009/02/11/Two-Lawyers-Fight-Cyber-Bullying.html?page=all.

This means that even after the harassment stops, an employer who Google searches a victim's name will still find all of the negative comments about the victim.

All three challenges could be addressed by holding ISPs liable for the harassment that occurs on their networks. The first challenge of finding the culprit would be addressed by holding the ISP liable because they have a fixed address and location. Victims would always have someone to hold responsible for the wrongs done to them. The second challenge of obtaining adequate relief would be addressed because ISPs generally have more money to pay for damages, and they are in a better position to defray costs to everyone by charging more for the services because of the increased liability. And the third challenge would be solved by requiring the ISP to remove offending material. As of now, section 230 of the CDA gives ISPs complete immunity.[96] ISPs have sole discretion as to whether they will remove harassing comments or assist in finding the actual harassers.

IV. Copyright Material on the Internet and How It Relates To Cyberharassment

Essentially, law makers drafting laws to protect against cyberharassment must determine who should bear the costs of cyberharassment. Currently, law makers have said that victims of cyberharassment should either internalize the harm of harassment, or try to sue the person who harmed them. The latter is almost impossible because section 230 has made the ISP not liable for any defamation made by a poster on their websites.[97] The laws governing use of copyrighted material on the internet has gone through a similar history as cyberharassment. Despite the

[96] Communications Decency Act, 47 U.S.C. § 230 (2000); *see also* Zeran v. America Online, Inc., 958 F. Supp. 1124 (E.D. Va. 1997), *aff'd*, 129 F.3d 327 (4th Cir. 1997).
[97] *Zeran*, 958 F. Supp. 1124.

similarities, ISPs have limited liability for subscriber copyright infringement, whereas ISPs are completely immune from liability for subscriber's defamatory comments.

A. History of Cyber-Copyright

The internet made sharing documents and files with the entire world easier than ever. Unfortunately, it also made illegally sharing copyrighted materials easier than ever, and it made it difficult for the owners of the copyright to enforce their rights. When a violation occurred, the owner of the copyright could sue the person who actually committed the infringement.[98] However, similar to cyberharassment, the infringer was often hard to find and usually judgment proof.[99] On the other hand, the ISP is much easier to find—they usually have a physical location—and the ISP has more money to actually pay for the violations.[100] Also, the ISP has the ability to remove the infringing content from the website and is in a better position to identify and find the actual infringer.[101] Because of these reasons, when copyrights started to be infringed on the internet, the owners of the copyrights looked for reasons to hold the ISP, as well as the infringer, liable for a violation.[102] The two theories of liability on which an ISP can be liable for its subscribers' copyright violations are direct liability and indirect liability.

The theory of direct liability for an ISP based on its subscriber's copyright violation is based on the idea that the ISP is providing the internet service to the infringing subscriber.[103] This is plausible because of the way file sharing on the internet works. Each time a subscriber

---

[98] G. Teran, *ISP Liability for Copyright Infringement*, HARVARD.EDU (Feb. 11, 1999), http://cyber.law.harvard.edu/property99/liability/main.html.
[99] V.K. Unni, *Internet Service Provider's Liability for Copyright Infringement - How to Clear the Misty Indian Perspective*, 8 RICH. J.L. & TECH. 13, ¶ 9 (Fall 2001) *available at* http://www.richmond.edu/jolt/v8i2/article1.html.
[100] *Id*.
[101] *Id*.
[102] *Id*.
[103] Alfred C. Yen, *Internet Service Provider Liability for Subscriber Copyright Infringement, Enterprise Liability, and the First Amendment*, 88 Geo. L.J. 1833, 1840-41 (2000).

uploads material to a web page, they instruct the ISP's computer to make and store a copy of the uploaded material.[104] "The ISP's computer then makes copies of the material every time a person views the subscriber's webpage and sends those copies through the internet to the viewing party.[105] Because the ISP's computers are making copies of copyrighted material, the ISP could theoretically be held directly liable for copyright infringement. This direct liability theory is supported by *Playboy Enterprises, Inc., v. Frena* but has been discredited by subsequent case law.[106]

In *Frena*, the defendant, George Frena, collected subscriptions and operated a Bulletin Board Service (BBS).[107] The subscribers could browse documents and photographs on Frena's computer through a modem.[108] The subscribers could also upload and download material from the BBS, which was essentially Frena's computer.[109] One of the subscribers uploaded an image to the BBS that was copyrighted by Playboy.[110] This means that Frena's computer, the BBS, was being used to store, copy, and distribute the Playboy image.[111] Playboy informed Frena about the image, and Frena removed the image immediately.[112] Frena claims he did not know about the image beforehand. Playboy still sued and won. The *Frena* court held that Frena was directly liable for the infringement. The court ruled that knowledge or intent was not a requirement of

[104] *Id*. at 1840.
[105] *Id*.
[106] Playboy Enterprises, Inc., v. Frena, 839 F. Supp. 1552 (M.D. Fla. 1993).
[107] *Id*. at 1554. "A BBS is an independently run computer system that allows users to dial in using a modem and terminal software. Once connected, the visitor can download files, read news, exchanges messages with other users or view other content provided on the BBS." A BBS was an ISP before the World Wide Web. *What Is A BBS?*, WISEGEEK (May 8, 2013), http://www.wisegeek.com/what-is-a-bbs.htm.
[108] 839 F. Supp. at 1554.
[109] *Id*.
[110] *Id*.
[111] *Id*.
[112] *Id*.

copyright.[113] The fact that Frena's computer was being used to copy and distribute copyrighted material meant that Frena was liable for copyright infringement. ""It does not matter that Defendant Frena may have been unaware of the copyright infringement."[114] Although Frena was a case involving a BBS operator, it is a simple step for judges to hold ISPs directly liable for copyright infringement once it is established that BBS operators are liable.

Other courts have refused to follow the *Frena* analysis and have held BBS operators not directly liable for their subscribers copyright infringement. In *Religious Technology Center v. Netcom On-Line Communication Services, Inc.*, Netcom was the ISP provider for a website.[115] One of its subscribers, Dennis Erlich, posted copyrighted material on the website.[116] The court rejected the *Frena* approach and held that Netcom would not be directly liable for the subscriber's infringement.[117] However, the court left open the idea that Netcom could be liable for a contributory infringement if they encouraged the subscriber to post the material.[118]

B. Enter the Digital Millennium Copyright Act

Similar to defamation under the Communication Decency Act, Congress recognized that courts were applying different standards of liability on ISP providers, which made it difficult for ISPs to know what they needed to do to avoid liability.[119] Congress attempted to address this confusion and enacted the Digital Millennium Copyright Act (DMCA).[120] The DMCA basically removes any direct liability an ISP would have for its "passive transmission, retransmission, or temporary storage of material through or on their networks" as long as the ISPs meet basic

[113] *Id*. at 1559.
[114] Playboy Enterprises, Inc., v. Frena, 839 F. Supp. 1552, 1559 (M.D. Fla. 1993).
[115] Religious Tech. Ctr. v. Netcom On-Line Commun. Serv., 907 F. Supp. 1361 (N.D. Cal. 1995).
[116] *Id*. at 1365-66.
[117] *Id*. at 1372.
[118] *Id*. at 1375.
[119] Alfred C. Yen, *Internet Service Provider Liability for Subscriber Copyright Infringement, Enterprise Liability, and the First Amendment*, 88 Geo. L.J. 1833, 1881 (2000).
[120] Digital Millennium Copyright Act, 17 U.S.C. § 512 (2006).

requirements.[121] The basic requirements are an ISP must adopt policies that terminate subscribers who are repeat offenders and must implement specific measures to protect the copyrighted material.[122] The issue of vicarious liability is a little more complicated. The issue that relates most to cyberharassment is the long term storage of infringing material, "such as hosting a web-page."[123] The ISP can avoid liability for a subscriber using the ISP's website to post copyrighted material if it:

> (A)(i) does not have actual knowledge that the material or an activity using the material on the system or network is infringing;
> (ii) in the absence of such actual knowledge, is not aware of facts or circumstances from which infringing activity is apparent; or
> (iii) upon obtaining such knowledge or awareness, acts expeditiously to remove, or disable access to, the material;
> (B) does not receive a financial benefit directly attributable to the infringing activity, in a case in which the service provider has the right and ability to control such activity; **and**
> (C) upon notification of claimed infringement as described in paragraph (3), responds expeditiously to remove, or disable access to, the material that is claimed to be infringing or to be the subject of infringing activity.[124]

Essentially, the ISP (A) cannot know about the infringement, (B) cannot have a financial interest in the infringing activity, and (C) must remove the infringing material once it is notified of its existence.[125] All three elements (A, B, and C) must be satisfied for the ISP to avoid liability.

There are two other requirements the ISP must do to avoid liability. First, the ISP must designate an agent to receive formal complaints about infringements; second, the ISP must follow the "prescribed method for handling those complaints."[126] When the designated agent receives a complaint from a copyright owner, the ISP must remove the offending material and

[121] Yen, 88 Geo. L.J. at 1881; *see also* 17 U.S.C. § 512(a).
[122] 17 U.S.C. § 512(a).
[123] Yen, 88 Geo. L.J. at 1881.
[124] 17 U.S.C. § 512 (emphasis added).
[125] 17 U.S.C. § 512.
[126] 17 U.S.C. § 512; Alfred C. Yen, *Internet Service Provider Liability for Subscriber Copyright Infringement, Enterprise Liability, and the First Amendment*, 88 Geo. L.J. 1833, 1848 (2000)

notify the ISP subscriber that the material was removed from the website.[127] The subscriber then has the opportunity to file a formal counter-notice with the ISP's designated agent challenging the validity of the removal of the material.[128] "A condition of that response's validity includes the subscriber's submission to jurisdiction in a United States District Court."[129] After the counter-notice, the ISP must provide the complainant with a copy of the counter-notice.[130] This gives the complainant the opportunity to file with a court a request for an order to restrain the subscriber from violating his copyright.[131] If the complainant does not respond, the ISP must restore the subscriber's material within 10 days.[132]

C. How Copyright Law Relates to Cyberharassment

Although copyright law is a strange place to search for potential solutions to cyberharassment challenges, there are many similarities between internet copyright law and cyberharassment laws. First, the history and development of internet copyright law closely mirrors cyberharassment. In cyberharassment, the courts tried to analogize existing defamation laws and apply them to situations involving the internet and the ISP. Although the ISP was never actually committing the infraction, plaintiffs attempted to hold them liable for the defamation of their subscribers. After several attempts and different rulings in each case, it became clear that existing defamation laws would not yield consisting and predictable rulings. Congress decided to step in and created a law that directly addressed the problem; the CDA held ISPs were not liable for the defamatory remarks made by their subscribers.[133]

---

[127] 17 U.S.C. § 512.
[128] 17 U.S.C. § 512.
[129] Yen, 88 Geo. L.J. at 1884-85; 17 U.S.C. § 512.
[130] 17 U.S.C. § 512.
[131] Alfred C. Yen, *Internet Service Provider Liability for Subscriber Copyright Infringement, Enterprise Liability, and the First Amendment*, 88 Geo. L.J. 1833, 1885 (2000).
[132] 17 U.S.C. § 512.
[133] *See supra* § IV.B.

Copyright law experienced an incredibly similar development. The invention of the internet created more and easier ways for people to violate someone's copyright. The courts, just like with defamation, tried to analogize regular copyright infringement to cyber copyright infringement. Again similar to defamation, plaintiffs tried to hold ISPs liable for their subscriber's infringement even though the ISP was not actually committing the violation. Just like in cyber-defamation, the courts had a difficult time articulating a consistent and predictable standard, which resulted in unpredictable results. Congress took notice and addressed the problem through the Digital Millennium Copyright Act. However, unlike cyber-defamation, Congress decided to hold the ISPs liable for their subscriber's copyright infringement unless the ISP met certain requirements.[134]

The history and development of the laws are not the only thing copyright infringement and cyber-defamation have in common. The two cyber-crimes share the challenges of enforcing the laws. Both crimes have difficulty finding the actual harasser or infringer.[135] Also, once the infringer is found, both types of crimes have difficulty in the perpetrators being judgment proof.[136] And the biggest challenge to both crimes is removing the offending/infringing material from the website.[137] The DMCA has been effective in addressing these issues regarding

---

[134] *See supra* § IV.B.

[135] *See* Danielle Keats Citron, *Cyber Civil Rights*, 89 B.U. L. REV. 61, 73 (2009) (discussing how the harassers used anonymizing software to hide their identity); *see also* V.K. Unni, *Internet Service Provider's Liability for Copyright Infringement - How to Clear the Misty Indian Perspective*, 8 RICH. J.L. & TECH. 13, ¶ 9 (Fall 2001) *available at* http://www.richmond.edu/jolt/v8i2/article1.html (discussing the difficulty in finding the infringer).

[136] *See* David Margolick, *Slimed Online*, UPSTART BUSINESS JOURNAL (Aug. 4, 2011), http://upstart.bizjournals.com/news-markets/national-news/portfolio/2009/02/11/Two-Lawyers-Fight-Cyber-Bullying.html?page=all (discussing how the victims only received 4 digit settlements); *see also* V.K. Unni, 8 RICH. J.L. & TECH. 13, ¶ 9 *available at* http://www.richmond.edu/jolt/v8i2/article1.html (discussing how the copyright infringers are usually judgment proof).

[137] *See* David Margolick, *Slimed Online*, UPSTART BUSINESS JOURNAL (Aug. 4, 2011), http://upstart.bizjournals.com/news-markets/national-news/portfolio/2009/02/11/Two-Lawyers-Fight-Cyber-Bullying.html?page=all; *see also* V.K. Unni, 8 RICH. J.L. & TECH. 13, ¶ 9 *available at* http://www.richmond.edu/jolt/v8i2/article1.html.

copyright infringement.[138] Because the issues facing copyright infringement are essentially the same as cyber-harassment, the DMCA should be used as a model to address the problems in current cyber-harassment laws.

V. Proposed Solution to Cyberharassment Laws

All of the challenges that cyberharassment laws currently fail to address could be addressed by holding ISPs liable for their subscribers' harassing comments. Since cyberharassment has so many similarities with copyright law, the Digital Millennium Copyright Act should work as a model to impose liability on ISPs. The main shortcoming of cyberharassment law is its inability to remove offending material from the internet once it is identified. Because this is the biggest concern, this legislative proposal will have that end goal in mind. In this proposal an ISP will be liable for the defamatory and harassing comments made by its subscribers unless the ISP, upon notification of claimed harassment or defamation, responds expeditiously to remove, or disable access to, the material that is claimed to be harassment or defamation.[139]

Just as under the DMCA, an ISP must have a designated agent to receive complaints and must remove the offending material upon complaint. Then the ISP must send a notice to the subscriber that his material has been removed and allow the subscriber to appeal it. If the subscriber appeals it, the ISP must notify the complainant and the complainant can then file suit against the appealing subscriber to determine if the material meets the elements of cyberharassment or defamation. If the subscriber files an appeal with the ISP and the complainant does not file suit against the subscriber, then the

[138] David Kravets, *10 Years Later, Misunderstood DMCA is the Law That Saved the Web*, WIRED (Oct. 27, 2008), http://www.wired.com/threatlevel/2008/10/ten-years-later/.
[139] This proposal is heavily borrowed from 17 U.S.C. § 512 (emphasis added).

subscriber's material will be put back up on the ISP's servers. If the subscriber does not appeal the complaint, then the material will remain removed from the ISP's servers.

Additionally, the ISP must take reasonable and good faith steps to be able to learn the identity of any of its subscribers who participate in defamation or harassment. Although the term "reasonable" is a vague term, the courts have experience in applying a reasonable standard and will have little trouble applying it to an ISP liability context.[140] In this context, reasonable will be what is technologically available to ISPs and not overly burdensome. The reasonableness of some steps to identify subscribers may be different for a small ISP and a large ISP because of the resources available to each. This part of the proposal will have to be examined by judges and a baseline of minimum requirements will be established. Two examples of steps an ISP can take to identify their subscribers is save the Internet Protocol (IP) address history of their subscribers and require subscribers to log-in before they can post anything on the website. The IP address can be used to identify who is accessing a particular webpage.[141] If ISPs were required to save its subscribers' IP address history, victims of cyberharassment could subpoena that information to try to identify the harasser. Also, requiring a person to log-in before making comments on a webpage would directly link a person's identity to their comments. Both of these suggestions are reasonable because some ISPs already keep IP address history[142] and some webpages already have the option to only comment if you are logged-in.[143]

---

[140] Vaughan v. Menlove, (1837) 132 Eng. Rep. 490 (first case to mention the reasonable man).
[141] *How To Find Someone Online Using Their IP Address*, HUBPAGES (May 6, 2013), http://glassvisage.hubpages.com/hub/How-to-find-people-online-by-their-IP-address.
[142] Ernesto, *How Long Does Your ISP Store IP-Address Logs?*, TORRENTFREAK (June 29, 2012), http://torrentfreak.com/how-long-does-your-isp-store-ip-address-logs-120629/.
[143] *Who Can Comment*, WORDPRESS.COM (May 6, 2013), http://en.support.wordpress.com/who-can-comment/.

Also, the ISP must take steps to prevent subscribers who habitually defame or harass from continued access to their website. There is no specific procedure that an ISP must follow to satisfy this requirement. However, one website, Craigslist, provides an example of an easy procedure that has helped reduce its spam levels. For someone to post an advertisement on Craigslist, that person must provide a valid phone number.[144] Once the number is provided, Craigslist calls the phone and gives the subscriber a verification number that the subscriber must enter into Craigslist before they can post anything.[145] If the content the subscriber posts is flagged and considered to be spam, then Craigslist removes the content and puts that phone number on a list of "invalid" phone numbers.[146] If the subscriber wants to post more material on Craigslist, they would have to provide a new phone number. This phone verification technique is one of many ways an ISP could prevent habitual offenders from having access to the ISP's website.

Here is a summary of what the requirements are for the proposed legislation to make ISPs liable for subscribers conduct. For an ISP to not be liable they must:

- Quickly remove any material that a person formally complains about;
- Set up a procedure that allows for complaints to be received and to notify subscribers that their material has been taken down;
- Have a system to identify anonymous subscribers; and
- Have a system to ensure habitual offenders are denied access to the ISP's websites.

[144] *Phone Authentication*, CRAIGSLIST (May 6, 2013), http://www.craigslist.org/about/help/phone_authentication.
[145] *Id*.
[146] Johnponting1, *A Tale About The Procedure of Phone Number Verification*, WORDPRESS.COM (Nov. 20, 2012), http://mr1numbercom.wordpress.com/2012/11/20/a-tale-about-the-procedure-of-phone-number-verification/.

A. How This Proposal Will Help Cyberharassment Victims

Currently, victims of cyberharassment have difficulty enforcing cyberharassment laws because the perpetrators can stay anonymous.[147] The ISPs have no incentive to either help the victims determine the identity of the perpetrators or remove the offending content because they are not liable under section 230.[148] However, eliminating ISP immunity in defamation and harassment cases will shift ISP incentives. Just like the DMCA has cut down on copyright infringement, a similar limited liability for ISPs regarding defamation will cut down on cyberharassment.[149] As discussed earlier, cyberharassment laws have three main weaknesses as currently constructed. First, and most important, the victim has no ability to remove the harassing material from the internet. Second, it is difficult to actually find the harasser because the internet makes it easy to stay anonymous. Third, even if the victims do find their harasser, the harasser usually does not have much money.[150] Thus, the victim is not adequately compensated. Concededly, this proposal does not fully address the third issue of the victim not being adequately compensated. However, it does fully address the first two issues.

1. Victim's Ability to Remove Offending Material

This proposal directly addresses the biggest weakness in current cyberharassment law: the removal of harassing material from the internet. Because this proposal hinges ISP liability on whether the ISP quickly removes the offending material, the victim has a quick and effective avenue to remove harassing material. And if the ISP decides not to remove the material, at least the victim has someone they can sue. Also, this proposal does not overburden ISPs with impossibly high requirements. ISPs can easily comply because they only have to remove content

[147] *See supra* § II.
[148] Communications Decency Act, 47 U.S.C. § 230 (2000).
[149] David Kravets, *10 Years Later, Misunderstood DMCA is the Law That Saved the Web*, WIRED (Oct. 27, 2008), http://www.wired.com/threatlevel/2008/10/ten-years-later/.
[150] *See supra* § II.

when it is brought to their attention. Currently, this basic proposal is being applied by every ISP and has been very successful.[151] YouTube, for example, allows for subscribers to upload their own videos to YouTube's servers. Subscribers upload 72 hours of video per minute.[152] At that rate, it would be virtually impossible to monitor every video upload for copyright infringement. However, YouTube quickly removes any video after receiving a complaint.[153] YouTube created a webpage where a copyright owner can easily submit a complaint.[154] Without the ability to avoid liability through DMCA compliance, YouTube would not exist because it would be impossible to monitor every video for copyright infringement.[155] The DMCA has been in effect for over ten years, and ISPs have had little trouble complying with the requirement to remove content upon notice, and copyright holders have been able to remove illegal content quickly and easily.[156] Because defamation law has so many similarities with copyright law, this similar proposal of notice and removal should be equally as effective to the rights of cyberharassment victims, without unduly burdening the ISPs.

The DMCA has been helpful to ISPs and copyright holders but some critics think the DMCA has infringed on the subscriber's ability to post information.[157] The DMCA requires an ISP to immediately remove content upon notification.[158] The ISP cannot take into account the merit of the complaint. Because of this immediate removal requirement, there have been abuses

---

[151] David Kravets, *10 Years Later, Misunderstood DMCA is the Law That Saved the Web*, WIRED (Oct. 27, 2008), http://www.wired.com/threatlevel/2008/10/ten-years-later/.
[152] *Statistics*, YOUTUBE (May 6, 2013), http://www.youtube.com/yt/press/statistics.html.
[153] *Frequently Asked Copyright Questions: Why Was My Video Was Removed, But Similar Ones Weren't?*, YouTube (May 6, 2013), http://www.youtube.com/yt/copyright/faq.html.
[154] *Copyright Infringement Notification Basics*, YOUTUBE (last visited May 6, 2013), http://www.youtube.com/yt/copyright/copyright-complaint.html
[155] David Kravets, *10 Years Later, Misunderstood DMCA is the Law That Saved the Web*, WIRED (Oct. 27, 2008), http://www.wired.com/threatlevel/2008/10/ten-years-later/.
[156] *See generally Id*.
[157] *Id*.
[158] Digital Millennium Copyright Act, 17 U.S.C. § 512 (2006).

by copyright holders.[159] Some copyright holders request the ISP to remove the material even though it does not infringe on their copyright.[160] This type of abuse can limit free expression. If cyberharassment law adopted the same standard of removal as the DMCA, there would be some abuse of the process and it would infringe on the subscriber's free expression. However, this problems was recognized when passing the DMCA.[161] The DMCA was an attempt at "carefully balancing the interests of both copyright owners and users."[162] The current laws governing cyberharassment protects the ISPs and does not attempt to balance the rights of the victims. Under this proposal free expression might be slightly impaired. However, this infringement will be small compared to the benefits the victims of cyberharassment will receive. Just like the DMCA, this proposal will attempt to balance the rights of the victims with the free expression rights of the people, while continuing to promote the growth of the internet.

2. Victim's Ability to Find Their Harasser

This proposal also directly addresses ISPs role in finding the identity of the actual perpetrator. This proposal would require ISPs to institute reasonable and good faith steps to find the identity of its subscribers.[163] Although the actions required by the ISPs to comply with this step of the proposal are unclear, several possibilities include saving IP addresses and requiring a subscriber to log-in before posting material to the internet. While a subscriber can take simple steps to cover their identity, this requirement might help some victims.[164] Some people will not hide their identity. For these situations, the victim can subpoena the ISPs records and identify

---

[159] David Kravets, *10 Years Later, Misunderstood DMCA is the Law That Saved the Web*, WIRED (Oct. 27, 2008), http://www.wired.com/threatlevel/2008/10/ten-years-later/.
[160] *Id*.
[161] President's Statement on Signing the Digital Millennium Copyright Act, 2 Pub. Papers 1902 (Oct. 28, 1998) *available at* http://www.presidency.ucsb.edu/ws/?pid=55169.
[162] *Id*.
[163] *See supra* § V.
[164] *How Do You Hide Your IP Address?*, HOWSTUFFWORKS (May 6, 2013), http://www.howstuffworks.com/internet/basics/hide-ip-address.htm.

their harasser. After the victim identifies the harasser, the victim can sue the harasser and recover money for her damages. Also, the harasser may be less inclined to continue to harass the victim once his identity is discovered.

B. How This Proposal Accords With Congressional Intent of The Communications Decency Act

Since Congress has already addressed the issue of online defamation, it is important to consider whether this new proposal contradicts any of Congress's original intentions in passing the Communications Decency Act. Congress's main objective in passing the Communications Decency Act was to overrule *Stratton v. Prodigy*.[165] In overruling *Prodigy*, Congress wanted to create an atmosphere that encouraged the growth and development of the internet.[166]

Arguably, this proposal advances the objective of promoting growth and development of the internet. In 2006, a study showed that individuals writing on the internet with a female name received 25 times more malicious and sexually threatening comments than authors with male names.[167] According to one study, an 11% decline in woman's use of chat rooms can be attributed to menacing comments.[168] Some people have argued that cyberharassment has led to some women either limiting their online presence or leaving the internet conversation completely.[169] This new proposal would allow more protection for people who are experiencing cyberharassment. This extra protection would, hopefully, encourage people who would otherwise stay offline to contribute to the market place of ideas on the internet. This extra

[165] H.R. CONF. REP. NO. 104-458, at 194 (1996).
[166] Joel R. Reidenberg et al., *Section 230 of the Communications Decency Act: A Survey of the Legal Literature and Reform Proposals*, CENTER ON LAW AND INFORMATION POLICY, Apr. 25, 2012 at 8.
[167] Robert Meyer & Michel Cukier, ASSESSING THE ATTACK THREAT DUE TO IRC CHANNELS, IN PROCEEDINGS OF THE INTERNATIONAL CONFERENCE ON DEPENDABLE SYSTEMS AND NETWORKS 467 (2006).
[168] *See Female Bloggers Face Harassment*, WOMEN IN HIGHER EDUC., June 2007, at 5.
[169] Danielle Keats Citron, *Law's Expressive Value In Combating Cyber Gender Harassment*, 108 Mich. L. Rev. 373, 385 (2009).

contribution would arguably enrich the internet community and would continue to promote the development of the internet.

However, even if this proposal contradicts Congress's original intent of the CDA, the CDA has outlived its purpose. The CDA was an attempt to balance the rights of individuals with the goal of developing the internet.[170] Creating an atmosphere for unfettered growth of the internet may have been important in 1996 when the CDA was passed, but now the internet is a strong element of our society. In 1996 about 1% of the world population was using the internet.[171] Today nearly 40% of the world's population is using the internet.[172] The internet is now fully developed and will survive limited liability imposed on ISPs. Laws are trending towards increasing restrictions and disincentives for internet growth. One example is sales tax on merchandise sold on the internet. Currently, there is no consistently enforced sales tax on internet sales.[173] When Congress passed the Internet Tax Freedom Act of 1998, eliminating sales tax for internet sales, their goal was to encourage the growth of the internet.[174] Congress thought that a state tax system on internet sales would be too burdensome and prevent the survival of the industry.[175] Congress is currently considering a bill that would repeal the state internet sales tax ban.[176] The internet is mature enough that it does not need special treatment to survive and grow. Congress no longer needs to promote the unfettered growth of the internet, and ISP limited liability for subscriber cyberharassment would give victims real relief while barely inhibiting the continued growth of the internet.

---

[170] Zeran v. America Online, Inc., 958 F. Supp. 1124, 1135 (E.D. Va. 1997).
[171] *Internet Growth Statistics*, INTERNET WORLD STATS (May 6, 2013), http://www.internetworldstats.com/emarketing.htm
[172] *Id*.
[173] Internet Tax Freedom Act of 1998, 47 U.S.C. § 151 (2013).
[174] Jerry Johnson, *Extension of the Internet Tax Nondiscrimination Act*, TAXADMIN.ORG, P. 3 (May 22, 2007), *available at* http://www.taxadmin.org/fta/rate/IFTA_FTA_test2.pdf.
[175] *Id*.
[176] The Marketplace Fairness Act, H.R. 684, 113th Cong. (2013).

VI. Conclusion

Cyberharassment is a serious crime with very serious, real world effects on the victims. Victims feel scared, embarrassed, and it can ruin their online reputation. Many states have directly addressed cyberharassment in statutes, however, true relief for the victims is impossible because ISPs have complete immunity from liability for their subscriber's cyberharassment. Victims cannot remove the harassing or defaming material from the web, thus continuing the harm the victims suffer well after the initial harassment has ended. However, Congress has already addressed a similar issue, internet copyright, which can be used as a model to improve the current cyberharassment law. By applying the DMCA to cyberharassment, the law will give victims of cyberharassment the means to remove the offending material from the internet and the tools to find the cyberharasser.