4-1-2010

Cyberharassment: A Call to Federal Action

Nick Peterson

Follow this and additional works at: https://scholarsarchive.byu.edu/byuplr

BYU ScholarsArchive Citation

This Article is brought to you for free and open access by the All Journals at BYU ScholarsArchive. It has been accepted for inclusion in Brigham Young University Prelaw Review by an authorized editor of BYU ScholarsArchive. For more information, please contact scholarsarchive@byu.edu, ellen_amatangelo@byu.edu.
CYBERHARASSMENT: A CALL TO FEDERAL ACTION

by Nick Peterson*

I. INTRODUCTION

On May 15, 2008, 49-year-old Missouri resident Lori Drew was summoned before a federal grand jury in connection with the suicide of 13-year-old Megan Meier. Drew, the girl’s neighbor, was accused of creating a fake MySpace profile of an attractive 16-year-old boy named Josh, supposedly to gain Megan’s trust and to discover what she was saying about Drew’s daughter online. Megan began an Internet relationship with Josh, but after a number of weeks his tone changed. Affection suddenly turned into invective as “Josh” unleashed a barrage of nasty comments and cruel bulletin posts, culminating in this final pronouncement: “You are a bad person and everybody hates you. Have a sh[---]y rest of your life. The world would be a better place without you.”1 Minutes later, Megan hung herself in her closet.

In time, the news of Megan’s death and the Internet hoax spread throughout the country. After local prosecutors could not find laws under which to charge Drew, the U.S. Attorney’s Office in Los Angeles charged Drew with violating MySpace’s Terms of Use.2 Drew

---

* Nick Peterson is a philosophy student from the Washington, D.C., area, anticipating graduation in April of 2011.


was convicted by the jury on the highly controversial grounds of violating the Computer Fraud and Abuse Act, but she was subsequently acquitted by a federal judge. With no existing legislation in place to specifically address cyberharassment, Drew was not judged according to her questionable dealings with Megan, but according to violation of an agreement with a website.

The nation’s legal system is not equipped with the proper legislation to handle such a case as United States v. Lori Drew, nor will it be until serious acts of cyberharassment are defined and prohibited. Although free speech must be protected on the Internet, the vicious communication that characterizes serious acts of cyberharassment should not be considered protected speech; because this behavior can be so severe, and because it is a significant nation-wide problem, federal legislators should prohibit serious acts of cyberharassment and provide oversight of the enforcement of such law.

II. THE PROBLEM OF CYBERHARASSMENT

Megan was a victim of what is now termed “cyberharassment,” an emerging form of harassment that impacts people throughout the nation. Cyberharassment, also termed “cyberbullying,” is defined as “willful and repeated harm inflicted through the use of computers, cell phones, and other electronic devices.” The two terms are generally used synonymously, although cyberbullying often concerns minor-to-minor interaction and cyberharassment usually refers to acts committed by adults. With the relatively recent advent of the Internet and the lack of legal direction and court precedent, cyber-

4 U.S. Const. amend. I, § 1.
5 Sameer Hinduja & Justin W. Patchin, Bullying Beyond the Schoolyard 5 (Corwin Press 2009).
6 For the purposes of this paper, the terms cyberbullying and cyberharassment will be used interchangeably.
harassment at present remains largely unchecked. Thus, victims are often left without effectual recourse, and most perpetrators remain undeterred and unpunished.

Cyberharassment can take the form of harassment, defamation, threat of harm, infliction of emotional distress, invasion of privacy, public disclosure of confidential information, and so on. Of the various forms of cyberharassment, many instances of such behavior would constitute actionable conduct when committed via non-electronic communication. Such acts may result in considerable harm, including substantial loss of self-esteem, loss of reputation, humiliation, severe emotional and physical damage, and even suicide. While other cases may not be as severe, Megan’s suicide demonstrates how damaging—even deadly—cyberharassment can be.

A few recent instances of cyberharassment in Missouri are perhaps more typical cases of such behavior. In the first application of Missouri’s new cyberharassment law, a 40-year-old woman was charged with felony harassment for posting a 17-year-old girl’s photo, address, and other personal contact information on Craigslist’s “Casual Encounters” section, a supposed “prank” which could have had frightening consequences for the girl. Another adult woman was charged with harassing a 17-year-old girl by sending a number of lewd and threatening text and voice messages, some of which threatened rape, after hearing that the girl had a physical encounter with

8 See Hinduja, supra note 5, at 35-41.

9 Id. at 42.

10 This cyberharassment prohibition, adopted in the wake of Megan Meier’s death, could set an important precedent for state and federal cyberharassment legislation.

the woman’s boyfriend. These cases illustrate the reckless, even dangerous behavior that can be associated with cyberharassment.

Furthermore, the victimization entailed in cyberharassment is quite a different matter from traditional harassment and, in some ways, more troubling. The very nature of electronic communication (particularly over the minimally regulated domain of the Internet) creates an environment for perpetrators seemingly free of repercussions. This perception of invisibility significantly “undermines the impact of the potential for a negative consequence administered by an authority or through social disapproval...[and makes] it easier to rationalize an irresponsible or harmful action.”

Perpetrators not only feel safe from exposure, they also do not have to see their victims suffer. Without the “tangible feedback of face-to-face interaction...[perpetrators] are distanced from a perception of the harm that their behavior has caused. The lack of tangible feedback undermines feelings of remorse...[and] makes it easier to rationalize an irresponsible or harmful action.” Thus, the impersonality of such electronic correspondence drastically lowers social inhibitions. Moreover, the near-universal accessibility of the Internet enables offenders to strike at almost anyone from almost any location. All of these factors combine to make electronic communication lend itself to brazen, harmful, thoughtless acts of harassment and abuse.

Over the last decade, because of the increasing prevalence of electronic communication, the problem of cyberharassment has grown significantly. In 2006, a survey commissioned by the National Crime Prevention Council found that “slightly more than four in ten teens (43%) report[ed] that they have experienced some form
of cyberbullying in the last year.”\textsuperscript{16} A similar survey by Hinduja and Patchin found nearly identical results.\textsuperscript{17} Furthermore, cyberharassment is also a growing issue among adults and in the workplace.\textsuperscript{18} Regardless of the venue of the harassment or the ages of those involved, such behavior can result in irreparable damage; in fact, although the circumstances surrounding Megan’s suicide are more extreme than most cases of cyberharassment, several other recent suicides have been directly linked to cyberharassment.\textsuperscript{19} People across the nation are at risk, and without significant reforms this problem will only worsen in this society of steadily increasing electronic interaction.

III. THE CONTROVERSY OF UNITED STATES V. LORI DREW

The case of United States v. Lori Drew exposes a legal system ill-prepared to handle cyberharassment. Although Drew’s actions ignited an uproar of opposition because of the highly controversial grounds of Drew’s charges, this case has also sparked a great deal of criticism.\textsuperscript{20} However, when allegations against Drew became public, it was clear that Drew’s behavior at least warranted legal scrutiny. A fraudulent MySpace account had been created to lure, deceive,


\textsuperscript{19} Hinduja, supra note 5, at 66-68.

and manipulate Megan; humiliation and emotional damage were inflicted that ultimately resulted in Megan taking her own life. Despite all of this, with no cyberharassment legislation in place, local attorneys could not find any substantial criminal charges with which to prosecute Drew.\textsuperscript{21} It took a federal grand jury in California to convict Drew of violating website policy for any legal scrutiny of her questionable behavior to ensue.\textsuperscript{22}

Without cyberharassment laws or court precedent, U.S. Attorney Thomas O’Brien charged Drew with violating the Computer Fraud and Abuse Act by breaching MySpace’s Terms of Use Agreement, which requires users to provide truthful information about themselves, to refrain from soliciting personal information from minors, and to refrain from using MySpace services to harass or harm other people.\textsuperscript{23} Initially the jury found Drew guilty, but after an appeal in a federal appellate court, U.S. District Judge George Wu dismissed all charges against her—stating in his opinion that “If any violation of any term of service is [enough] to make the access unauthorized...it would...render the statute incredibly overbroad” (emphasis added).\textsuperscript{24} Judge Wu recognized that convicting Drew would have had clearly chilling implications for the country’s Internet-using population—many of whom likely never read a word of the fine print before clicking “I Agree.”

The charges against Drew are not only highly questionable, but they do not strike at the heart of the issue: with this approach, the victim was not Megan but MySpace, and the charge against Drew was not cyberharassment but violation of a tenuous website agreement. The issue at hand, however, is not the culpability of Drew’s actions. The problem is that, with no cyberharassment legislation in place, there is still no way to even determine the guilt or innocence of Drew’s most significant actions. Without public policy directly related to cyberharassment, loosely-relat-

\begin{itemize}
\item \textsuperscript{21} \textit{Zetter, supra} note 2.
\item \textsuperscript{22} \textit{Id}.
\item \textsuperscript{23} MySpace.com Terms or Use Agreement, http://www.myspace.com/index.cfm?fuseaction=misc.terms (last visited Feb. 22, 2010).
\item \textsuperscript{24} United States v. Lori Drew, 259 F.R.D 449 26 (2009).
\end{itemize}
ed legislation was stretched far outside of intended bounds, and thus, the seriousness of Drew’s actions escaped examination.

IV. THE NEED FOR LEGISLATION

Present Internet policy and harassment laws do not provide victims of cyberharassment with sufficient opportunity for redress. At present, most victims have three main options: they may (1) confront the harasser in person, (2) report the harasser to the Internet Source Provider (ISP), or (3) pursue civil litigation. The first option is clearly inadvisable in many circumstances and could likely exacerbate the issue. Of the second option, if the ISP does actually take any action, at most it will only revoke accounts, remove comments, shut down websites, or respond with other such measures. This does not significantly deter perpetrators, who can easily set up another account under a different name and resume antagonism.

Most victims of serious cyberharassment are left with one remotely feasible option: civil litigation. However, while this may be a viable option for some cases of cyberharassment, present harassment tort law is not designed to apply specifically to electronic media. Non-electronic harassment and electronic harassment should be treated separately and distinctly, just like harassment in person and over the telephone currently are; the behavior may be essentially the same in certain respects, but the medium carries with it considerably different social ramifications and implications (i.e., the Internet is the only social domain where one can be completely anonymous; also, offenders are not limited by proximity to the victim, nor are they deterred by the fear of confronting authorities). As a result of these distinctions, civil or criminal non-electronic harassment policy does not apply well to the open domain of the Internet.

Furthermore, civil law cannot account for instances of cyberharassment that are criminally severe in nature. In some circumstances, “cyberbullying rises to the level of criminal behavior,” for

example, when it involves a viable threat of physical harm. While many instances of cyberbullying may fall short of deserving criminal classification, some more exceptional, vicious, and harmful circumstances may warrant criminal prohibition. To illustrate this distinction, consider different acts of telephone harassment. A single petty prank call is often more of a passing irritation than a criminal act. However, when an individual targets another with malicious intent and begins a pattern of harassing, obscene, or threatening phone calls, the offender abandons the bounds of protected speech and trespasses into the territory of criminal behavior. Such is the case with cyberharassment; just because most instances of electronic communication should be protected does not mean that criminal behavior over an electronic medium should go unpunished.

V. FEDERAL LEGISLATION AND ENFORCEMENT

In April of 2009, Representative Linda T. Sanchez (D-California) proposed a federal Bill against cyberbullying titled the Megan Meier Cyberbullying Prevention Act. Of the proposed legislation, Sanchez stated that “without a federal law [prohibiting] cyberbullying...cyber bullies are going unpunished....This bill sends a clear message to anyone who commits cyberbullying: online actions will have severe offline consequences.” On September 29, 2009, the bill was sent to the House of Representatives Subcommittee on Crime,

26 Hinduja, supra note 5, at 180.
Terrorism, and Homeland Security where it has remained since.\textsuperscript{30} The proposed cyberbullying law reads as follows:

(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.\textsuperscript{31}

Although this bill is a step in the right direction, it has come under a lot of fire since its introduction to the House. The major concern most critics have with Representative Sanchez’s bill is that it would infringe upon protected speech rights. Professor Eugene Volokh, a renowned and outspoken defender of free speech, argues, “The law, if enacted, would clearly be facially overbroad (and probably unconstitutionally vague), and would thus be struck down on its face under the First Amendment.”\textsuperscript{32} Admittedly, in its present state,


\textsuperscript{31} H.R. 1966, \textit{supra} note 28.

some of the bill’s language is problematic and overly vague, and it does not convey the intent to uphold protected speech.

To improve the wording of the proposed bill, changes such as the following ought to be enacted: (1) the bill should address the overarching behavior of cyberharassment, rather than simply cyberbullying (to make it clear that this legislation is not only related to minors); (2) speech should be liable only when it meets certain specific qualifications beyond a reasonable doubt (e.g., the speech is transmitted with malicious intent, has no legitimate purpose, would likely induce emotional distress or fear of physical harm in any reasonable person in the same circumstances, and so on); (3) the particular venues of the speech may require different standards (i.e., speech on public blogs and websites may be viewed differently from more private means, such as email, text messages, instant messages, and so on); and (4) the punitive measures should be differentiated between minor-to-minor behavior and behavior involving adults. There are likely other ways in which the language of the legislation could be improved, but changes such as these would help narrow the bill’s scope.

In the words of Representative Sanchez from a recent House committee hearing, it is important to recognize “how difficult it will be to craft a prohibition on cyberbullying that is consistent with the Constitution.” However, with changes such as, but not limited to, those mentioned above, her legislation would reflect her desire to create a law that “distinguish[es] between an annoying chain email, a righteously angry political blog post, or a miffed text to an ex-boyfriend—all of which are and should remain legal...and serious, repeated, and hostile communications made with the intent to harm.” Such a law could enable attorneys and officials to discern between harmless and harmful instances of electronic communication and could clearly prohibit serious acts of cyberharassment.

This position, however, prompts the following question: where does one cross the lines between harmless teasing, significant harassment, and criminal behavior? The answer, as with many legis-

33 Sánchez, supra note 30.
34 Id.
lated issues, lies in legal definition and case-by-case judgment. For a sexual harassment claim to be actionable, certain qualifications must be met; the same is true with libel, hate speech, obscenity, and other such tortious and criminal behavior. Federal legislators can explore the issue and prescribe rules or tests with which to determine whether cyberharassment behavior warrants legal prosecution. Law enforcement and government officials would be responsible to use good judgment to apply such criteria to the actions of those charged. With such measures in place, legislation can be broad enough to be effective, and yet narrow enough to avoid infringing on free speech rights, thus bringing justice to both victims and perpetrators.

In addition, federal legislators should provide for federal oversight over the enforcement of such law. One way to implement enforcement of cyberharassment legislation would be to house it under the Department of Justice’s (DOJ) section on Computer Crime and Intellectual Property. Within this section of the DOJ, the Internet Crime Complaint Center (IC3) was established to provide avenues of reporting Internet crimes and to provide for analysis and pursuit of such claims. The IC3 offers the following procedure:

IC3’s mission is to serve as a vehicle to receive, develop, and refer criminal complaints regarding the rapidly expanding arena of cyber crime. The IC3 gives the victims of cyber crime a convenient and easy-to-use reporting mechanism that alerts authorities of suspected criminal or civil violations. For law enforcement and regulatory agencies at the federal, state, and local level, IC3 provides a central referral mechanism for complaints involving Internet related crimes.35

Similar reporting and enforcing measures used to combat other forms of Internet crime could be adopted to address cyberharassment. While not all cases will amount to actionable behavior, the injured party will at least be instructed on how to proceed and ad-

dress the issue. To avoid being inundated with petty claims or false accusations, the DOJ may have to establish qualifications with which to sift through the claims to find those that are legitimate and viable. With this information in mind, however, the purpose of this paper is not to specify every particular of the implementation of federal law and enforcement, but to demonstrate that there may already be organizations and systems in place that handle cyber crime that could be adjusted to confront the national problem of cyberharassment.

VI. Responding to Objections

Potential critics might argue that cyberharassment legislation could unduly limit free speech. While such rights must be upheld, the government ought to ensure the protection and well-being of its citizens. In the case of severe cyberharassment, the protection of the health and safety of American citizens should supersede the protection of senseless, hostile speech. Boundaries should be set for language employed solely to degrade, denigrate, and endanger the innocent. As briefly mentioned above, telephone harassment is separately treated and federally criminalized by the Communications Act. This addendum to the U.S. Code makes placing telephone calls “with intent to annoy, abuse, threaten, or harass another person” a federal offense worthy of a hefty fine or up to two years imprisonment.\(^{36}\) Since the federal government deems it necessary to protect the safety and well-being of its citizens from unreasonable telephone harassment, it is reasonable to expect such protection from similar (or even more serious) behavior over the Internet or other electronic media.

Furthermore, in recent years legislators have expanded the scope of the U.S. Code’s stalking prohibition to encompass electronic media. The statute now states that if any person “uses the mail, any interactive computer service, or any facility of interstate or foreign commerce to engage in a course of conduct that causes substantial emotional distress to that person or places that person in reasonable fear of the death of, or serious bodily injury,” then that person is

\(^{36}\) 47 U.S.C § 223 (2008).
guilty of a federal offense. While the intent of this prohibition is to address the specific behavior of cyberstalking, a similar prohibition of cyberharassment seems an intuitive extension of the same reasoning behind this prohibition of stalking over electronic media. In fact, criminalizing serious acts of cyberharassment may even avert patterns of behavior that might develop into more dangerous patterns of cyberstalking.

The issue of cyberharassment legislation is especially controversial because it involves governmental regulation of free speech over the Internet, something many people oppose. The ACLU, for example, maintains that the “government should not be in the business of deciding what we all can and cannot see or do on the Internet. Those decisions are for all of us to make, and for all parents to make, not for [the] government to make.” While the government has largely taken a sort of laissez-faire approach to online speech, there are certain cases in which the government—in the interest of the well-being of its citizens—has regulated free speech on the Internet. For example, the Federal Trade Commission is authorized to protect consumers from deceptive commercial speech and practices online. Of the FTC’s mission, Acting Director Eileen Harrington stated the following:


38 See Parry Aftab, Understanding The Cyberharassment Problem, InformationWeek, 23 Aug. 2004, http://www.informationweek.com/news/security/privacy/showArticle.jhtml?articleID=29116706 (last visited Feb. 22, 2010) (Aftab, the executive director of WiredSafety.org, stated the following in drawing a distinction between cyberharassment and cyberstalking: “Cyberstalking is almost always characterized by the stalker relentlessly pursuing his or her victim online and is much more likely to include some form of offline attack, as well. This offline aspect makes it a more serious situation as it can easily lead to dangerous physical contact if the victim’s location is known.”).

The [FTC’s] Bureau of Consumer Protection works to protect consumers against unfair, deceptive, or fraudulent practices in the marketplace. The Bureau conducts investigations, sues companies and people who violate the law, develops rules to protect consumers, and educates consumers and businesses about their rights and responsibilities. The Bureau also collects complaints about consumer fraud and identity theft and makes them available to law enforcement agencies across the country.40

Thus, this federal agency regulates and restricts Internet speech to protect consumers’ financial interests. Similar legal justification for FTC Internet fraud and safety policy should be extended to Internet harassment. Not only do citizens deserve protection from harmful speech in the commercial realm of the Internet, but they also deserve protection in the social realm of electronic communication.

With all of this in mind, it doesn’t mean that teasing, name-calling, or appropriate public venting should be criminalized; intuitively, language that could be spoken out loud without legal repercussion should not be penalized merely because it is typed. However, behavior that would be tortious or even criminal in the case of non-electronic communication should be prohibited online as well. While some demeaning and derogatory language may be protected as opinion under the freedom of speech on or offline, behavior that is senseless, malicious, severely harassing, or clearly threatening should be prohibited regardless of the particular medium of communication involved.

Potential critics of federal cyberharassment legislation might also argue that the problem should simply be dealt with on the state and local level. However, cyberharassment is a nation-wide problem unbound by state and local lines—thus it should be addressed uniformly throughout the country. In the years since cyberharassment has surfaced as a serious issue, only a handful of states have adopted legislation that directly prohibits cyberharassment; most state cyberbullying measures merely direct schools to establish cyberbullying

While schools should take action against cyberharassment within their own spheres of influence, most cases of cyberharassment happen off school property and out of the hands of school administrators. Moreover, cyberharassment is not simply an issue of disrupting the school environment, but it can be a matter of severe harassment and denigration for youth and adults alike. The existing sparse patchwork of public policy will not suffice in providing victims with recourse, bringing offenders to justice, or deterring potential cyberharassers.

Furthermore, while cyberharassment predominately happens between acquaintances, it can also happen between strangers and across state boundaries. The 2006 survey commissioned by the National Crime Prevention Council found that 41% of victims were unaware of the perpetrators’ identities or locations, many of whom may have been in different states from their victims. All else aside, the simple fact that this behavior can cross state lines mandates that, if it is criminalized throughout the country, federal measures must be in place for when it does become an interstate matter. The Internet is a public, national domain not easily divisible by state boundaries; this does not mean that states should refrain from establishing clear prohibitions of cyberharassment, but it means that this issue often involves multiple states. If each state adopts different and even conflicting cyberharassment laws, how can our legal system aptly address conflicts of interstate communication? Just as the federal government has established its jurisdiction over interstate Internet commerce and our nation’s telephone network, so too should cyberharassment be dealt with on the federal level.

---

41 Hinduja, supra note 17.
VII. Conclusion

Cyberharassment occurs throughout the nation’s electronic networks, and it is time for federal legislators to take action against this problem. However, the purpose of this paper is not to claim that federal legislation is the silver bullet for cyberharassment, nor to claim that this issue should not be addressed by state legislatures. As with many other laws, a certain degree of overlap between federal and state measures can ensure that this problem is dealt with thoroughly and effectively. While such measures will take care of the most serious cases, many instances of cyberharassing behavior will likely fall short of warranting criminal investigation and prosecution. Nevertheless, federal legislation will lay the foundation for the nation’s fight against Internet harassment. Without federal consensus and legislation, people do not know how to confront cyberharassment; they are uncertain about the limits of free speech, and about when and how to seek legal redress. With such legislation, state officials, law enforcement, educators, and parents will be prompted to consider this issue and to adopt more specific policies to prevent more victims from sharing Megan’s fate. Cyberharassment can be combated, and through federal legislation the federal government can and should lead the way.