Santa Clara High Technology Law Journal

Volume 17 | Issue 1 Article 4

January 2001

Cyberstalking: Can Communication via the Internet Constitute a Credible Threat and Should an Internet Service Provider Be Liable if It Does?

Joanna Mishler

COMMENTS

Cyberstalking: Can Communication via the Internet Constitute a Credible Threat and Should an Internet Service Provider Be Liable if it Does?

Joanna Lee Mishler[†]

TABLE OF CONTENTS

I. INTRODUCTION

You are in the privacy of your home, relaxing after a long day at work. Suddenly you hear a knock at the door. "Who is it?" you ask. The man behind the door responds by saying he has a package for you. You see no need to be alarmed, so you slowly open the door, curious about the contents of the package. As soon as you open the door, the man pushes you to the floor, starts ripping off your clothes and rapes you. According to this guy, *you* asked for it. "*Honestly*," he says, "I was following the directions you posted on the Internet!"

While such a scenario seems far-fetched, it happens more often than we think. In fact, this story is based on a real case in California.[1]

[†] B.A., Telecommunications, Indiana University, 1997; J.D. Candidate, Santa Clara University School of Law, 2001.

[1] *See* Gina Keating, *Man Gets Maximum Sentence For Cyber Stalking of Woman He Met at Church*, CITY NEWS SERVICE, July 22, 1999, *available at* LEXIS, News Library, City News

For months, several men visited a 28-year old California woman and attempted to carry out the above scenario.[2] The perpetrators all later claimed they had seen her name, phone number and address on the Internet prompting them to go to her home seeking sexual relations.[3] Six men came to the victim's apartment.[4] Some claimed they had seen "steamy e-mails" sent in her name.[5] One message read: "Tell me you have a package, and when I open my door, attack me. Tie me, gag me, rip off my clothes and go for it. I'll struggle a little just for the fun of it . . . ."[6]

The Internet postings were later discovered to have originated from a man whom the victim had previously met and later rejected.[7] The man, later identified as Gary S. Dellapenta, was apprehended and given the maximum sentence for the crime.[8] Ironically, Dellapenta's victim did not have Internet access in her home.[9] For sometime, she did not even know why the men were targeting her.[10] Eventually, the victim's father contacted her stalker posing as someone interested in the elaborate rape fantasy.[11] This action, along with the help of a police investigation, led to Dellapenta's arrest.[12] In April 1999 Dellapenta pled guilty to three counts of solicitation for sexual assault and one count of stalking.[13] The judge sentenced him to six years in state prison, stating "to give him anything less is insufficient to protect society."[14]

In another real-life situation, a woman found a message posted on the Internet, listing her home phone number, her address and a message that read "[she] was available for sex anytime of the day or

---

Service File.

[2] *Id.*

[3] *See id.*

[4] *Id.*

[5] *Id.*

[6] *Id.*

[7] Keating, *supra* note 1.

[8] *See id.*

[9] *See id.*

[10] *Id.*

[11] *See id.*

[12] *Id.*

[13] Keating, *supra* note 1.

[14] *Id.* Television dramas tend to mimic news stories like this one. For example, in an episode of the television show *Nash Bridges*, one of the female characters experienced a similar encounter. *Nash Bridges: Vendetta* (CBS television broadcast, Apr. 23, 1999). However, the show differed in that the victim not only knew her stalker, but was the detective who had helped send the stalker to prison for beating up his wife years earlier. *Id.* The fictitious stalker's motive was a clear case of revenge. *Id.*

night."[15] After being plagued by numerous phone calls, the woman contacted the local, county and state authorities, as well as the FBI asking for help.[16] The woman testified that "[t]hey all looked at me and said, '[w]e have no idea how to help you.'"[17]

In another case, Kevin Massey, who stalked a founder of a Dallas Internet Service Provider (ISP), actually called himself the 'Cyberstalker' and lobbied to be a guest on Howard Stern's radio show.[18]

The U.S. Department of Justice (DOJ) defines *stalking* as: "harassing or threatening behavior that an individual engages in repeatedly, such as following a person, appearing at a person's home or place of business, making harassing phone calls, leaving written messages or objects, or vandalizing a person's property."[19] Stalking is not a new problem; the Internet has simply provided a new and more anonymous medium for the same old crime.[20] This new crime has been aptly labeled *cyberstalking* and has been defined as "use of the Internet, e-mail or other electronic communications devices to stalk another person through threatening behavior."[21]

Using new technologies, stalkers can now reach victims in their homes, a place where one usually feels safe. Even more disturbing, cyberstalkers can stalk entirely from the comfort of their own home.[22] Due to the ease of electronic communication, users may feel that sending another user a potentially threatening e-mail is harmless compared to traditional stalking. For example, an Internet user may send a threatening e-mail to another user, not realizing the e-mail could eventually end up in a public forum. Such a prank can lead to harmful and humiliating consequences, as in the case of Internet user

---

[15] Jonathan Karl, *Congress Urged to Strengthen Anti-Stalking Laws, Include Internet*, CNN.COM *at* http://www.cnn.com/US/9909/29/internet.stalking/ (Sept. 29, 1999).

[16] *Id.*

[17] *Id.*

[18] *See* Kevin Whitelaw, *Fear and Dread in Cyberspace*, U.S. NEWS & WORLD REP, Nov. 4, 1996 at 50.

[19] OFFICE OF JUSTICE PROGRAMS, U.S. DEP'T OF JUSTICE, STALKING AND DOMESTIC VIOLENCE, THIRD ANNUAL REPORT TO CONGRESS UNDER THE VIOLENCE AGAINST WOMEN ACT 5 (1998).

[20] Jessica Laughren, *Cyberstalking Awareness and Education, at* http://www.acs.ucalgary.ca/~dabrent/380/webproj/jessica.html (last visited Oct. 31, 1999).

[21] Sunny Sea Gold, *V.P. Al Gore Visits SDSU*, THE DAILY AZTEC, *at* http://www.dailyaztec.com/Archive/Fall-1999/09-20/city/city01.html (Sept. 20, 1999).

[22] *Why Does Cyber-Stalking Occur as Often as it Does?*, CYBERANGELS.ORG, *at* http://www.cyberangels.org/stalking/often.html (last visited Jan. 26, 2000) ("Cyberstalking is also much easier to practice than IRL stalking—in cyberspace a stalker can harass their target without ever having to leave the comfort of their own home.").

Bryan Winter.[23] Winter "wrote the archetypically arrogant male brushoff e-mail, setting off a firestorm of urban myth and electronic revenge."[24] He sent a degrading e-mail to a woman he had met in a bar, arrogantly rejecting her desire to meet with him again.[25] Seeking revenge, the woman forwarded the e-mail to all of her friends.[26] Ultimately, Winter's seemingly private message became a very public chain e-mail that can now be found on at least one website.[27]

Despite this new medium, most states do not have anti-stalking laws that explicitly cover cyberstalking.[28] The law in California, which was used in the prosecution of Dellapenta,[29] was only recently amended with language to cover cyberstalking.[30]

Most articles addressing cyberstalking focus on actions taken via e-mail, a one-on-one private forum. This comment will focus on cyberstalking conducted in public forums, rather than personal e-mail. Part II provides a background of traditional anti-stalking laws and the evolution of cyberstalking law. The California Penal Code currently provides a traditional anti-stalking law, which technically includes cyberstalking.[31]

Part III discusses how the traditional anti-stalking laws should be modified to accommodate activity on the Internet. Specifically, Part III focuses on the meaning of a *credible threat* requirement[32] found in modern anti-stalking laws, and proposes that such a requirement be eliminated. The credible threat requirement is outdated because the Internet allows a cyberstalker to maintain physical distance whereas traditional stalking necessarily involved contact between the stalker and the intended victim.

---

[23] Gentry Lane, *The Humiliation Of Bryan Winter, at* http://www.salon.com/health/sex/urge/1999/05/11/bryan_winter/ (last visited Nov. 29, 2000).

[24] *See id.*

[25] *See id.*

[26] *See id.*

[27] *See id.*

[28] *See* U.S. Dep't of Justice, *1999 Report on Cyberstalking: A New Challenge for Law Enforcement and Industry, at* http://www.usdoj.gov/criminal/cybercrime/cyberstalking.htm (last visited Nov. 28, 1999).

[29] *See* Greg Miller, *Man Pleads Guilty to Using Net to Solicit Rape*, LOS ANGELES TIMES, Apr. 29, 1999 at C5.

[30] *See id. See also* CAL. PENAL CODE § 646.9 (West 1999 & Supp. 2000).

[31] *See* § 646.9.

[32] According to the cyberstalking watch group Cyberangels, "[o]ne interesting aspect of Credible Threat is that if you are threatened online, you have no way of knowing if the person can carry it out or not." *Policy Concerns About Cyberspace Stalking*, CYBERANGELS.ORG *at* http://www.cyberangels.org/stalking/law.html (last visited Jan. 26, 2000).

Finally, Part IV concludes by briefly considering ISP vicarious liability for cyberstalkers, in both the civil and criminal contexts. In the civil context, Congress has provided immunity for ISPs in most cases. This comment asserts that such immunity will likely extend to cyberstalking issues. In the criminal context, this comment contends that ISPs simply lack the requisite intent element required for the crime. Therefore, this article argues that a cyberstalker's ISP should not be held liable for its subscriber's actions.

II. BACKGROUND

> *Make no mistake: this kind of harassment can be as frightening and as real as being followed and watched in your neighborhood or in your home.* —Vice President Al Gore[33]

On July 18, 1989, Robert John Bardo shot and killed actress Rebecca Schaeffer in broad daylight.[34] Bardo used computer databases to find out her telephone number, where she lived, whom she called, the kind of car she drove and where she shopped.[35] In this highly publicized stalking case, Bardo used the computer to find information on Schaeffer long before the Internet had become popular.[36]

Shaeffer's murder brought about a heightened awareness of the problems involved when applying traditional anti-stalking laws to cyberstalking. In response, the California Legislature enacted Penal Code Section 646.9, a criminal anti-stalking law that provides in relevant part:

> (a) Any person who willfully, maliciously, and repeatedly follows or harasses another person and who makes a *credible threat* with the intent to place that person in reasonable fear for his or her safety, or the safety of his or her immediate family, is guilty of the crime of stalking.[37]

In the recent California case of *People v. Borrelli*, the Court of Appeal articulated a test for identifying violations under Section 646.9:

---

[33] *1999 Report on Cyberstalking*, *supra* note 28.

[34] Laughren, *supra* note 20.

[35] *Id.*

[36] *Id.* ("Bardo may have been physically distanced from his obsession but the computer electronically made him feel near to her.").

[37] CAL. PENAL CODE § 646.9 (West 1999 & Supp. 2000) (emphasis added).

> In order to be penalized under section 646.9, subdivision (a), the defendant must willfully engage in the prohibited conduct with the intention of inflicting substantial emotional distress on the person to whom the comments were directed in violation of the latter's constitutionally guaranteed rights to pursue safety, happiness, and privacy as guaranteed by our state and federal constitutions; the threats must be made with the apparent ability to carry them out so as to cause the person who is the target of the threat to reasonably fear for his or her safety; and the victim must actually suffer substantial emotional distress.[38]

When Section 646.9 was enacted, use of the Internet was not yet popular as a public forum for communication. As such, cyberstalking was practically unknown. Now, over 90 million people in the U.S. have Internet access, giving stalkers a new and more anonymous arena to perpetrate their crimes. According to the DOJ, "[g]iven the enormous amount of personal information available through the Internet, a cyberstalker can easily locate private information about a potential victim with a few mouse clicks or key strokes."[39] The Information Age has evolved since Schaeffer's murder and now stalkers can commit crimes on-line in a way that Bardo could only imagine.

Cyberstalking is specifically defined as "the use of the Internet, e-mail, or other electronic communications devices to stalk another person."[40] Cyberstalking can arise in two different forms: "(1) online cyberstalking and harassment that stays online, and (2) online harassment and stalking that ventures offline."[41] According to the House Judiciary Committee, "[a]lthough online harassment and threats can take many forms, cyberstalking shares important characteristics with offline stalking. Many stalkers—online or off—are motivated by a desire to exert control over their victims and engage in similar types of behavior to accomplish this end."[42] A typical stalking situation generally involves repeated harassing or threatening behavior, such as following a person, making harassing phone calls, leaving written messages or objects or vandalizing a person's property.[43] For example, law enforcement officers in California have encountered situations where victims repeatedly

---

[38] People v. Borrelli, 77 Cal. App. 4th 703, 716 (Ct. App. 2000).

[39] *1999 Report on Cyberstalking, supra* note 28.

[40] *See id.*

[41] Laughren, *supra* note 20 (emphasis added).

[42] H.R. REP. NO. 106-455, at 3-4 (1999).

[43] *1999 Report on Cyberstalking, supra* note 28.

receive the message '187' on their pagers.[44] The code '187' refers to the California Penal Code section covering homicide.[45] Similar to traditional stalking, cyberstalking usually involves a man stalking a woman.[46]

When the California legislature realized the need to adapt its anti-stalking law to address the increased use of high technology, it amended Sections 646.9(g) and (h) to encompass cyberstalking.[47] Subsections (g) and (h) were amended, "as measures designed particularly to address any harassment or credible threats made through electronic communications to another over the Internet or via computer network."[48] Section 646.9 now provides:

> (g) For the purposes of this section, 'credible threat' means a verbal or written threat, including that performed through the use of an *electronic communication device* . . . . It is not necessary to prove that the defendant had the intent to actually carry out the threat.
>
> . . . .
>
> (h) For purposes of this section, the term 'electronic communication device' includes, but is not limited to, telephones, cellular phones, computers, video recorders, fax machines, or pagers.[49]

This is the criminal anti-stalking law as it currently stands in California.

III. THE "CREDIBLE THREAT" REQUIREMENT IS OUTDATED

Dellapenta tormented his victim by posting her name and address on several web sites, soliciting other men to rape her.[50] In theory, most would probably agree that such on-line solicitation reaching

---

[44] *Id.*

[45] CAL. PENAL CODE § 187 (West 1999 & Supp. 2000).

[46] *See* Victim Profiles, CYBERANGELS.ORG, *at* http://www.cyberangels.com/stalking/victim.html (last visited Oct. 31, 1999); *see also* PATRICIA TJADEN & NANCY THOENNES, NAT'L INST. OF JUSTICE CTR. FOR DISEASE CONTROL AND PREVENTION, STALKING IN AMERICA: FINDINGS FROM THE NATIONAL VIOLENCE AGAINST WOMEN SURVEY, Apr. 1998, at 2 ("Although stalking is a gender-neutral crime, most (78 percent) stalking victims are female and most (87 percent) stalking perpetrators are male.").

[47] *See* Lisa A. Karczewski, *Stalking in Cyberspace: The Expansion of California's Current Anti-stalking Laws in the Age of the Internet*, 30 MCGEORGE L. REV. 517, 521 (1999); *see also* CAL. PENAL CODE § 646.9(g) (West 1999 & Supp. 2000).

[48] Karczewski, *supra* note 47, at 521; *see also* CAL. PENAL CODE § 646.9(g).

[49] CAL. PENAL CODE § 646.9(g), (h) (emphasis added).

[50] *See* Keating, *supra* note 1.

millions of potential users is certainly threatening. However, when applied in practice, most state anti-stalking laws, including Section 649.6, require stalkers to make a *credible* or overt threat *to the victim.*[51]

In practice, the credible threat requirement is rarely met. Although stalking victims often experience a high level of fear, "[l]ess than half of all stalking victims are *directly* threatened by their stalkers."[52] Thus, without an overt credible threat, law enforcement has difficulty helping victims of stalkers.[53] According to the *Cyberangels* Website, "[i]n a country where even targets of real life stalking are still told by the Police: 'We are sorry, but we can't do anything unless you get physically attacked,' small wonder that the 'virtual crime' of cyberstalking gets even less respect."[54]

In its report on "Stalking in America," the National Institute of Justice Centers for Disease Control and Prevention proposes that the "'credible threat' requirement[s] should be eliminated from the definition of stalking in all state anti-stalking statutes."[55] The credible threat requirement creates two significant questions: First, must the victim know of the threat as it is being made; and second, how far does the stalker have to go to constitute a credible threat to his/her victim?

The first obstacle in dealing with the credible threat requirement is what ramifications does the requirement have when the victim is unaware that the threat exists? For example, in the Dellapenta case, the victim was unaware that Dellapenta was the source of the posted messages.[56] The overt behavior by the men who followed up on the postings was surely threatening, but was Dellapenta truly threatening her as well? If so, at what point did he cross the line? His actions might not actually constitute a credible threat as required by Section 649.6. On the other hand, Dellapenta's actions may have created a

---

[51] *See* TJADEN & THOENNES, *supra* note 46, at 7.

[52] *Id.* at 2 (emphasis added).

[53] *See* Jessica Lloyd-Rogers, *Law Enforcement Tries to Catch Up with Online Stalkers*, SILICON VALLEY/SAN JOSE BUSINESS JOURNAL, Oct. 24, 1997, *available at* http://www.bizjournals.com/sanjose/stories/1997/10/27/focus2.html.
Victims should take certain steps in order for the police to effectively help them: (1) File a police report, (2) *Demand* that the report be taken (3) Begin establishing a paper trail and (4) Add *every* new incident to the report on file at the police station. *Id.*

[54] *How Does Law Enforcement Fit in?*, CYBERANGELS.ORG, *at* http://www.cyberangels.org/stalking/lawenforce.html (last visited Jan. 26, 2000).

[55] *See* TJADEN & THOENNES, *supra* note 46, at 2.

[56] *See* Keating, *supra* note 1.

threat when he originally posted the messages. Alternatively, the threat might not have surfaced until Dellapenta's victim became aware of those postings.

Most recent California cases interpreting Section 646.9 have not involved cyberstalking but instead have considered traditional stalking where the victim knows that he or she is being threatened at the time of the stalker's activity.[57] However, in the California case *People v. Norman*, the court of appeal addressed the issue of a delay between the stalker's harassment and his victim's awareness of that harassment.[58] The *Norman* court rejected the defendant's argument that to be punishable under Section 646.9, the stalking must be contemporaneous with the fear of threat.[59] In *Norman*, the traditional celebrity-stalking situation occurred when Jonathan Norman staked out the home of famous Hollywood director Steven Spielberg while Spielberg and his family were out of the country.[60] At one point, while driving by Spielberg's house, Norman showed his friend "a photograph of Spielberg's head affixed to a photo of a naked male body."[61] Norman later told this same friend that he intended to break into Spielberg's home and rape him.[62] Norman frequented the residence several times and was eventually apprehended by one of Spielberg's security guards.[63] While still out of the country with his family, Spielberg was notified by the authorities that "Norman had the names of Spielberg's wife and children in his day planner, that he had been carrying handcuffs, duct tape and a box cutter, and that Norman had a record of prior assaultive conduct."[64]

---

[57] A brief survey of California cases brought under California Penal Code Section 646.9 turned up the following cases: *See* People v. Borrelli, 77 Cal. App. 4th 703, 709 (Ct. App. 2000) (reciting the fact that Victim knew defendant had firearms and ammunitions and was threatened when he called and told her "today was the day he was going to kill her."); *see also* People v. Ewing, 76 Cal. App. 4th 199, 203-04 (Ct. App. 1999) (stating the fact that after defendant told victim during a phone conversation, "You think you know karate, I'll kick your ass," victim called 911 because she was scared); *see also* People v. Andrews, 75 Cal. App. 4th 1173, 1175 (Ct. App. 1999) (stating that defendant left several voice mail messages, including, "If I have a jury trial . . . I will never be convicted because you are . . . all . . . mother-fuckers, the top of the mother-fuckers," and "you are asking for fucking problems."); *see also* People v. Hale, 75 Cal. App. 4th 94, 100 (Ct. App. 1999) (stating that the defendant called the victim on her cell phone and said, "You know I'm going to kill you when I see you, right?").

[58] People v. Norman, 75 Cal. App. 4th 1234 (Ct. App. 1999).

[59] *See id.* at 1239.

[60] *See id.* at 1236.

[61] *Id.*

[62] *Id.*

[63] *See id.* at 1236.

[64] People v. Norman, 75 Cal. App. 4th 1234, 1237 (Ct. App. 1999).

One factor the court used in finding a threat was that "by its current provision that stalking can occur by the use of an 'electronic communication device,' including a computer, the statute necessarily encompasses situations where there is a delay between the defendant's harassment and his victim's awareness of the defendant's conduct."[65] The decision indicates that courts recognize threats at the time they occur even if the victim does not learn of the threat until a later time. Under such an interpretation, a stalker like Dellapenta could be found guilty of stalking even though his victim did not see the threatening message until well after he posted it.

The second obstacle of the credible threat requirement is the interpretation and scope of the *threat, i.e.*, what constitutes a threat and how far does the stalker have to go? Since Section 646.9 punishes the mere utterance of words, it has "First Amendment implications, [and] must be narrowly directed only to truly dangerous threats, *i.e.*, those that sometimes are termed 'true threats.'"[66] In *People v. Falck*, the court interpreted the credible threat requirement to include, "a threat which on its face and in the circumstances in which it is made is so unequivocal, unconditional, immediate and specific as to the person threatened, as to convey a gravity of purpose and imminent prospect of execution."[67] However, "it is enough that the threat causes the victim reasonably to fear for her safety . . . and that the accused makes the threat with the intent to cause the victim to feel that fear."[68]

California courts are not alone in wrestling with the interpretation of 'credible threat.' In *United States v. Alkhabaz*, the Sixth Circuit interpreted the threat element from the point of view of the person *receiving* the threat.[69] In *Alkhabaz*, defendant Jacob Alkhabaz (*a.k.a.* Jake Baker) posted several messages on an Internet bulletin board that consisted of short stories about the rape, torture and murder of women. [70] Baker had also been recounting his rape fantasies in an e-mail exchange with another man known only as 'Gonda.'[71]

In the e-mail at issue in *Alkhabaz*, Baker described a fantasy involving a specific woman he knew from school, a woman known

---

[65] *Id.* at 1239.

[66] People v. Falck, 52 Cal. App. 4th 287, 296 (Ct. App. 1997) (quoting People v. Gudger, 29 Cal. App. 4th 310, 316 (Ct. App. 1994)).

[67] *Id.* at 295 (citing People v. Fisher 12 Cal. App. 4th 1556, 1559 (Ct. App. 1993)).

[68] *Id.* at 297 (citing People v. Carron, 37 Cal. App. 4th 1230, 1238-1240 (Ct. App. 1995)).

[69] *See* United States v. Alkhabaz, 104 F.3d 1492 (6th Cir. 1997).

[70] *See id.* at 1493.

[71] *See* JONATHAN WALLACE & MARK MANGAN, SEX, LAWS, AND CYBERSPACE 66 (1996).

only as Jane Doe in the case.[72] Specifically, Baker recounts in various e-mail messages and Usenet postings different scenarios where he rapes and mutilates Jane Doe.[73] In one story, Baker and his fictitious friend, Jerry, have broken into Jane Doe's apartment and forced her to take off all of her clothes.[74] Baker then narrates: "As she's fighting, . . . eyes wide with fear, Jerry and I strip . . . . Jerry and I tie her by her long brown hair to the ceiling fan, so that she's dangling in mid-air . . . . Drool and loud squeaks escape through her gag."[75] The story then continues with the men viciously raping and killing Jane Doe.[76]

Baker was indicted for five counts of violating of 18 U.S.C. § 875(c), which provides: "[w]hoever transmits in interstate or foreign commerce any communication containing any threat to kidnap any person or any threat to injure that person of another, shall be fined under this title or imprisoned not more than five years, or both."[77] The particular stories offered for the indictments were in the form of private e-mail and were not available to the public on the Internet.[78]

When the school officials who discovered the postings showed the stories to Jane Doe, "Doe was visibly shaken . . . . [She] felt threatened."[79] The threat requirement under 18 U.S.C. § 875(c) requires "proof that a reasonable person would have taken the defendant's statement as 'a serious expression of an intention to inflict bodily harm.'"[80] However, the court seemed to gloss over this definition and held that Baker's actions did not constitute a threat.[81] According to the court, "[a]t their core, threats are tools that are employed when one wishes to have some effect, or achieve some

---

[72] *See Alkhabaz*, 104 F.3d at 1497.

[73] *See id.* at 1497 n.1.

[74] *See id.*

[75] United States v. Alkhabaz, 104 F.3d 1492 (6th Cir. 1997).

[76] *See id.* at 1497-98.

[77] 18 U.S.C.A. § 875(c) (West 2000). This language is similar to that of the proposed amendment to 18 U.S.C. § 2261A, discussed *infra*. Therefore, an alternative to prosecuting a cyberstalker under the current state anti-stalking laws might be to prosecute under Section 875(c). For example, in the First Circuit case of *United States v. Freeman*, the defendant pleaded guilty to violating 18 U.S.C. § 975(c). United States v. Freeman, 176 F.3d 575, 575 (1st Cir. 1999). The Court reiterated the determination of threat under that statute as "'whether [the defendant] should have reasonably foreseen that the statement he uttered would be taken as a threat by those to whom it is made.'" *Id.* at 578 (quoting United States v. Whiffen, 121 F.3d 18, 21 (1st Cir. 1997)). However, an analysis of this statute is beyond the scope of this paper.

[78] *See Alkhabaz*, 104 F.3d at 1493.

[79] WALLACE & MANGAN, *supra* note 71, at 68.

[80] *Alkhabaz*, 104 F.3d at 1494.

[81] *See id.* at 1496.

goal, through intimidation."[82] The court held that to constitute a threat under 18 U.S.C. § 875(c):

> a communication must be such that a reasonable person (1) would take the statement as a serious expression of an intention to inflict bodily harm (the *mens rea*) and (2) would perceive such expression as being communicated to effect some change or achieve some goal through intimidation (the *actus reas*).[83]

Applying the above rule to the case, the court concluded the private e-mail between Baker and Gonda did not contain a threat because a reasonable person would not "perceive such communications as being conveyed to effect some change or achieve some goal through intimidation."[84] In other words, Baker's friend was the recipient of the e-mail, and that message was sent to him as "an attempt to foster a friendship;" it was not meant as a threat to Gonda.[85] The court found that since Baker did not mean for Jane Doe to see this e-mail, she could not have been threatened by it.

The U.S. District Court in Oregon, on the other hand, has interpreted the threat requirement in a different manner.[86] In *Planned Parenthood v. American Coalition of Life Activists*, the court articulated an objective test that analyzed the threat *from the standpoint of the person making the threat*:

> [W]hether a reasonable person would foresee that the statement would be interpreted by those to whom the maker communicates the statement as a serious expression of intent to harm or assault . . . . [A]lleged threats should be considered in light of their entire factual context, including the surrounding events and the reaction of the listeners.[87]

In *Planned Parenthood*, the plaintiffs brought an action for injunctive relief and damages against anti-abortion activists.[88] The defendants had posted what they called the "Nuremberg Files" on the Internet.[89] This posting included dossiers on abortion doctors and read:

---

[82] *Id.* at 1495.

[83] *Id.*

[84] *Id.* at 1496.

[85] *Id.*

[86] *See* Planned Parenthood v. Am. Coalition of Life Activists, 23 F. Supp .2d 1182 (D. Or. 1998).

[87] *Id.* at 1189 (citation omitted).

[88] *See id.* at 1185.

[89] *See id.* at 1187.

> One of the great tragedies of the Nuremberg trials after WWII was that complete information and documented evidence had not been collected so many war criminals went free or were only found guilty of minor crimes. We do not want the same thing to happen when the day comes to charge abortionists with their crimes.[90]

The court held that this type of communication was actionable as a threat to the plaintiffs.[91]

Congress responded to this evolution of cyberstalking by leaving out the credible threat requirement from a proposed amendment to the federal anti-stalking law. On May 19, 1999, Representative Sue W. Kelley of New York introduced *The Stalking Prevention and Victim Protection Act of 1999* (H.R. 1869) to the House of Representatives.[92] The House passed the measure.[93] If passed by the Senate and signed into law by the President, the measure would amend the federal anti-stalking statute (18 U.S.C. § 2261A) to read, in relevant part:

> (b) For purposes of this section, a person stalks an individual if that person engages in conduct—
>
> (1) with the intent to injure or harass the individual; and
>
> (2) that places the individual in reasonable fear of the death of, or serious bodily injury (as defined for the purposes of section 2119) to, that individual, a member of that individual's immediate family (as defined in section 115), or that individual's intimate partner.[94]

A major catalyst for this amendment was the rise of cyberstalking.[95] During the debate on the House floor, California

---

[90] *Id.* at 1187-88.

[91] *Id.* at 1194.

[92] *See* 145 CONG. REC. E1028-03 (May 19, 1999), 1999 WL 317779.

[93] *See* H.R. 1869, 106th Cong. (1999). H.R. 1869 was passed by the House of Representatives on November 10, 1999, and sent to the Senate the same day. 145 CONG. REC. H11910-01 (Nov. 10, 1999) (statement of Rep. Bachus), 1999 WL 1020606.

[94] *See* H.R. 1869. The current law provides in relevant part:

> Whoever travels across a State line or within the special maritime and territorial jurisdiction of the United States with the intent to injure or harass another person, and in the course of, or as a result of, such travel places that person in reasonable fear of the death of, or serious bodily injury . . . to, that person or a member of that person's immediate family . . . shall be punished . . . .

18 U.S.C.A. § 2261A (West Supp. 2000).

[95] Representative Kelley's findings were based in part on a report generated by the Department of Justice on cyberstalking which had made the following recommendations:

> States should review their laws to determine whether they address cyberstalking and if not, expand the laws to do so. Federal law should be amended to prohibit the transmission of any communication in interstate or foreign commerce with

Representative Edward Royce stated, "these are instances where these individuals let their intent be known. They publish their threats against these victims. There is no reason why we cannot let law enforcement act upon those threats before it is too late, before these victims lose their lives."[96]

The purpose and summary section of H.R. 1869 notes that it will make several significant changes or additions to current law.[97] One such change is that "it would expand federal jurisdiction over stalking to reach stalkers who use the mail or any facility in interstate or foreign commerce to stalk their victims."[98] In other words, a cyberstalker could be federally prosecuted when he or she used the Internet to stalk because the Internet instantaneously crosses interstate lines.

More importantly, as stated above, H.R. 1869 does not have language requiring a credible threat. Instead, the measure requires "intent to injure or harass the individual . . . that places the individual in reasonable fear of the death of, or serious bodily injury."[99] When introducing H.R. 1869, Representative Kelly stated, "by criminalizing 'threatening behavior' as opposed to 'the demonstration of specific threats' this bill closes a loophole commonly used by accused stalkers to avoid conviction."[100]

The language proposed in H.R. 1869 would solve the timing issues as applied to Dellapenta's case because it does not require that victims ever know why their attackers are showing up or the contents of Dellapenta's communication on the Internet. Subsection (1) of H.R. 1869 was satisfied when Dellapenta posted the messages in an effort to hurt his victim and subsection (2) was satisfied when, as result of his posting, Dellapenta's victim was placed in fear of bodily injury each time a man came to her home to rape her. Moreover, H.R. 1869 solves the second obstacle of credible threat by completely eliminating the requirement altogether.

Still, as noted by Representative Spencer Bachus during the debate, "the vast majority of stalking cases are, and even after this

---

intent to threaten or harass another person where such communication places that person in reasonable fear of death or bodily injury . . . .

H.R. REP. NO. 106-455 (Nov. 5, 1999).

[96] 145 CONG. REC. H11910-01 (Nov. 10, 1999) (statement of Rep. Royce), 1999 WL 1020606.

[97] H.R. REP. NO. 106-455.

[98] *Id.*

[99] H.R. 1869.

[100] 145 CONG. REC. E1028-03 (May 19, 1999) (statement of Rep. Kelly), 1999 WL 317779.

legislation passes, will be prosecuted at the State and local level."[101] Therefore, it is up to individual states to provide language that will protect potential victims. The DOJ has been working on a *Model Antistalking Code* for the States.[102] This Model explicitly eliminates the credible threat requirement.[103] According to the DOJ:

> Stalking defendants often will not threaten their victims verbally or in writing but will instead engage in conduct which, taken in context, would cause a reasonable person fear. The model code is intended to apply such 'threats by implied conduct.' Therefore, the 'credible threat' language, which might be construed as requiring an actual verbal or written threat, was not used in the model code.[104]

By eliminating the need for a credible threat, the *Model Antistalking Code* makes prosecuting a cyberstalker more manageable. Therefore, the California legislature should amend Penal Code Section 646.9 with language similar to the *Model Antistalking Code* to make it clear to cyberstalkers, and to the courts, that *any* threatening behavior will not be tolerated.

IV. ISPs SHOULD NOT BE HELD LIABLE FOR SUBSCRIBER'S ACTIONS

> *One major ISP receives approximately 15 complaints per month of cyberstalking, in comparison to virtually no complaints of cyberstalking just one or two years ago.*[105]

Arguably, the next step in the evolution of cyberstalking might be to hold a cyberstalker's ISP liable for allowing its subscriber to harass and stalk others. For example, ISP liability may arise from a real-life cyberstalking incident that resulted in the death of the stalker's target.[106] On October 15, 1999, Liam Youens walked into a dentist's office, shot and killed Amy Boyer, then turned the gun on himself.[107] In what appears to be a typical cyberstalking incident, Youens used the Internet to find information about his victim and then dedicated an

---

[101] 145 CONG. REC. H11910-01 (Nov. 10, 1999) (statement of Rep. Bachus), 1999 WL 1020606.

[102] NAT'L INST. OF JUSTICE, U.S. DEP'T OF JUSTICE, DOMESTIC VIOLENCE, STALKING, AND ANTISTALKING LEGISLATION, ANNUAL REPORT TO CONGRESS, APP. B (Mar. 1996), *available at* http://www.ojp.usdoj.gov/ocpa/94Guides/DomViol/appendb.htm (last visited Nov. 8, 1999).

[103] *See id.*

[104] *Id.*

[105] *1999 Report on Cyberstalking*, *supra* note 28, at 6.

[106] *See Killer Plotted Murder Through Internet*, S.F. CHRON., Nov. 30, 1999, at A12.

[107] *See id.*

entire web site to an on-line chronicle of his obsession with Boyer.[108]

According to the San Francisco Chronicle, "Youens' thoughts and plans are detailed in a police report drawn partly from the web sites where he debated with himself whether to kill Boyer, kill another former classmate or storm into Nashua High School and kill as many people as he could."[109] A detailed excerpt from Youens' web site revealed, "[i]n the last 4 years I have had 3 or 4 dreams about Amy, but in the last month I've dreamt about her every single night . . . . The last dream I had Amy was pregnant, so I stabed [sic] the fetus through her, then cut her throat."[110] In addition to devoting his web site to an obsession with Boyer, Youens also used Internet search agencies to find her social security number and her address.[111]

In the aftermath of this incident Boyer's stepfather considered filing a lawsuit against one of Youens' ISPs, a company called Tripod.[112] Pursuant to an inquiry, a Tripod official stated that "almost no one visited Youens' site and that the company would have told the police had it known about the site."[113] Once law enforcement notified Tripod of the situation, the ISP took Youens' site off-line.[114] In a case like Boyer's where the cyberstalker makes Internet postings available to the public, a stalking victim might be inclined to sue the cyberstalker's ISP on the theory it should have known about the site and should have prevented its subscriber from maintaining such a site.

However, Congress provides ISPs immunity from civil liability in 47 U.S.C. § 230(c), which provides in relevant part:

> (1) Treatment of publisher or speaker. No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider.
>
> (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

---

[108] *See id.*

[109] *Id.*

[110] J.M. Hirsch, *Chilling Web Site Reveals a Killer's Obsessive Plans*, L.A. TIMES, Dec. 5, 1999 at A1.

[111] *Id.*

[112] *See Killer Plotted Murder Through Internet*, *supra* note 106.

[113] *Id.*

[114] *See id.*

> 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).[115]

The ISP immunity provided by 47 U.S.C. § 230(c) is generally applied in cases involving defamation, libel and slander causes of action.[116] Moreover, Congress explicitly provides in Section 230(e)(1) that this immunity will not necessarily apply in criminal cases.[117] Therefore, while the immunity provided by Section 230 protects ISPs from civil liability, protection from criminal liability remains unclear.

The Fourth Circuit addressed ISP civil liability under Section 230 in *Zeran v. America Online, Inc.*, refusing to extend liability to American Online (AOL) for the actions of its subscriber.[118] In *Zeran*, Plaintiff Kenneth Zeran brought a civil action against AOL alleging that AOL "unreasonably delayed in removing defamatory messages posted by an unidentified third party, refused to post retractions of those messages, and failed to screen for similar postings thereafter."[119] At that time, an earlier version of federal immunity for ISPs existed, similar to the current Section 230.[120]

In *Zeran*, another Internet user had posted a message on an AOL bulletin board falsely claiming Zeran was selling shirts that featured "offensive and tasteless slogans" relating to the Federal Building bombing in Oklahoma.[121] The posting included Zeran's home phone number.[122] As a result of the posting, Zeran received numerous death threats.[123] Zeran repeatedly notified AOL of this inaccurate posting, and asked that the posting be removed.[124] Somehow a posting with

---

[115] 47 U.S.C.A. § 230(c) (West Supp. 2000).

[116] *See, e.g.*, Lunney v. Prodigy Services Co., 723 N.E.2d 539, 543 (N.Y. 1999); Zeran v. Am. Online, Inc., 129 F.3d 327 (4th Cir. 1997).

[117] *See* 47 U.S.C.A. § 230(e)(1) (West Supp. 2000). This subsection specifically provides, "Nothing in this section shall be construed to impair the enforcement of section 223 or 231 of this title, chapter 71 (relating to obscenity) or 110 (relating to sexual exploitation of children) of Title 18, or any other Federal criminal statute." *Id.*

[118] *See Zeran*, 129 F.3d at 327.

[119] *Id.*

[120] The portion of 47 U.S.C. § 230 relevant to this issue had identical language to the current Section 230: "No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider." 47 U.S.C.A. § 230(c)(1) (West Supp. 2000).

[121] *See Zeran*, 129 F.3d at 329.

[122] *See id.*

[123] *See id.*

[124] *See id.*

his phone number remained on the AOL bulletin board and he continued to receive threatening phone calls.[125] In this case, AOL clearly knew about the problem and even assured Zeran the perpetrator's account would be closed.[126] However, the court still did not find AOL liable because Congress shielded ISPs from liability under the Communications Decency Act of 1996.[127]

Zeran is a typical defamation case brought against an ISP and, therefore, may be distinguished from a case wherein the subscriber takes on the identity of another Internet user. For example, an ISP might know that one of its subscribers runs a site on which many people post sexual fantasies. Depending on the nature of the fantasy, when the person posting the message is the person who has the fantasy this situation might not be a problem.[128] The problem arises when an Internet user takes on someone else's identity, such as when Dellapenta posted messages posing as his victim.[129] When testifying before Congress regarding Dellapenta, Deputy Attorney General Eric Holder stated:

> Current federal law does not address those situations where a cyberstalker uses unwitting third parties to bombard a victim with messages, transmits personal data about a person—such as the route by which the victim's children walk to school—in order to place such person or his family in fear of injury, or send an e-mail or other communications under someone else's name with the intent to abuse, harass, or threaten that person.[130]

The DOJ report on cyberstalking also discusses this situation:

> [A] cyberstalker can dupe other Internet users into harassing or threatening a victim by utilizing Internet bulletin boards or chat rooms. For example, a stalker may post a controversial or enticing message on the board under the name, phone number, or e-mail address of the victim, resulting in subsequent responses being sent to the victim. Each message—whether from the actual cyberstalker or others—will have the intended effect on the victim, but the cyberstalker's effort is minimal and the lack of direct contact between the cyberstalker and the victim can make it difficult for

---

[125] *See id.*

[126] *See id.*

[127] Zeran v. Am. Online, Inc., 129 F.3d 327, 329 (4th Cir. 1997).

[128] However, a situation similar to the Jake Baker case discussed in Part III, would pose the typical cyberstalking problem. *See* United States v. Alkhabaz, 104 F.3d 1492 (6th Cir. 1997).

[129] *See* Keating, *supra* note 1.

[130] *Cyberattack Investigation: Congressional Testimony*, Feb. 29, 1999, 2000 WL 11068569 (testimony of Deputy Att'y. Gen., Eric Holder).

law enforcement to identify, locate, and arrest the offender.[131]

Considering these potential problems, should the ISP require some sort of consent from those participating, in case the posting is not what it seems? Should the ISP then be liable if it does not get that consent?

The New York Court of Appeals considered liability of an ISP for the actions of a subscriber in such a case.[132] In *Lunney v. Prodigy Services Company*, the plaintiff alleged that his ISP (Prodigy) was negligent because it did not employ safeguards to prevent an imposter from opening on-line accounts in the plaintiff's name.[133] An imposter had opened an on-line account in the name of Plaintiff Alexander Lunney and had used that account to post vulgar messages on a Prodigy bulletin board.[134] The court noted that electronic bulletin boards pose "more complicated legal questions" than e-mail communication; therefore operators have a greater level of cognizance over them.[135]

The court first held that Prodigy was not a publisher in this situation.[136] The court then addressed Lunney's allegation that the ISP failed to prevent the imposter from opening the account.[137] According to the court, "[Plaintiff] would require an ISP to employ a 'process for verification of the bona fides' of all applicants and any credit cards they offer so as to protect against defamatory acts."[138] The defendant ISP argued that such a duty "would require an ISP to perform investigations on millions of potential subscribers, so as to be guarantors against harmful transmissions."[139] The court agreed, stating:

> [t]he rule plaintiff advocates would, in cases such as this, open an ISP to liability for the wrongful acts of countless potential tortfeasors committed against countless potential victims. There is

---

[131] *1999 Report on Cyberstalking, supra* note 28.

[132] Lunney v. Prodigy Services Co., 723 N.E.2d 539 (N.Y. 1999).

[133] *See id.*

[134] *See id.*

[135] *Id.* at 542 ("In many respects, an ISP bulletin board may serve much the same purpose as its ancestral version, but uses electronics in place of plywood and thumbtacks. Some electronic bulletin boards post messages instantly and automatically, others briefly delay posting so as not to become 'chat rooms,' while still others significantly delay posting to allow their operators an opportunity to edit the message or refuse posting altogether.").

[136] *Id.*

[137] *Id.* at 543.

[138] Lunney v. Prodigy Services Co., 723 N.E.2d 539, 543 (N.Y. 1999).

[139] *Id.*

> no justification for such a limitless field of liability. If circumstances could be imagined in which an ISP would be liable for consequences that flow from the opening of false accounts, they do not present themselves here.[140]

The Sixth Circuit addressed another situation wherein an imposter took on the identity of someone else in a print publishing context in *Ashby v. Hustler Magazine, Inc.*[141] In *Ashby*, Plaintiff Ursula Ashby brought an action for libel and invasion of privacy against defendant Hustler Magazine alleging that "the publication of her nude photograph in the magazine without her consent caused her to suffer severe emotional distress with resulting physiological consequences."[142] Ashby alleged that another woman had stolen nude pictures of Ashby, which had been taken for her private use.[143] In February 1981 Hustler received those pictures of Ashby from a woman claiming to be Ashby, along with a signed consent form.[144] A representative from Hustler called the woman who had sent the picture to verify she was in fact Ashby (the woman in the picture).[145] After seemingly verifying the identity of the woman, Hustler mailed her fifty dollars for the picture and published it in the June 1981 issue of *Hustler*.[146]

The Sixth Circuit court found Hustler liable, in part, because "Hustler's verification procedures were not, in any way, calculated to ensure that the person who had mailed the photograph and executed the release form was indeed the individual depicted in the sexually explicit photograph."[147] A factor in the court's decision was that since Hustler is known as a "tasteless and offensive" magazine, it had a higher duty of care.[148] While the *Ashby* example is not directly on point, it shows how a court may treat a situation that involves an Internet web site posting fantasies as described above.

Despite the immunity offered through Section 230, there may be another way to hold the ISP liable for the actions of its subscribers. According to the DOJ report on cyberstalking, "[ISPs] almost

---

[140] *Id.* (citation omitted).

[141] Ashby v. Hustler Magazine, Inc., 802 F.2d 856 (6th Cir. 1986).

[142] *Id.* at 858.

[143] *See id.* at 857.

[144] *See id.*

[145] *See id.*

[146] *Id.* at 858.

[147] Ashby v. Hustler Magazine, Inc., 802 F.2d 856, 859 (6th Cir. 1986); *see also* Wood v. Hustler Magazine, Inc., 736 F.2d 1084 (5th Cir. 1984).

[148] *Ashby*, 802 F.2d at 858-59.

uniformly have provisions in their online agreements specifically prohibiting abusive or harassing conduct through their service and providing that violations of the policy will result in termination of the account."[149] This type of a subscriber agreement works in theory, but realistically, ISPs are not actually capable of sifting through the thousands of new web sites that pop up on the Internet every day in order to discover violations. Once a subscriber sets up a web site, it can be readily modified at a moment's notice.

Since web sites can be modified frequently, ISPs do not have the resources to perpetually monitor the content of subscriber's web sites. Moreover, the courts consider ISPs analogous to telephone companies, immune from the content they deliver; therefore, "it is unlikely that they [ISPs] will have the incentive to monitor private e-mail."[150] With current technology, ISPs are just not equipped to read every message that passes through their systems. Should an ISP that knows about a certain questionable web site be held responsible for checking the site periodically to verify it is not breaking any laws? Since updating a web site can happen almost instantaneously, continuous monitoring is just not a reasonable option at this time. Therefore, at this point, ISPs should not be held civilly liable for their subscriber's actions.

However, in an ironic case regarding ISP liability, a defendant tried to blame AOL for enabling him to commit offensive acts because of the "anonymous availability provided by AOL chatrooms."[151] During Defendant Mottos' sentencing hearing, he argued that AOL is totally immune and is aware of the "garbage" that goes through cyberspace and "snares the Paul Mottos of the world."[152] He further argued, "[AOL] could shut down its vile chat rooms with the flick of a switch but with immunity and swollen cash registers it allows weak people to get ever weaker in their [sic] privacy of their home."[153] The court rejected this argument, stating:

> It is equally difficult to see how AOL's role as 'enabler' should even be a mitigating factor within the applicable sentencing range. As we would not mitigate the sentence of another sex offender who, say, read with interest The Story of O or The Story of Juliette, so we do not mitigate in Motto's case because of the

---

[149] *1999 Report on Cyberstalking, supra* note 28.

[150] David K. McGraw, *Sexual Harassment in Cyberspace: The Problem of Unwelcome E-mail*, 21 RUTGERS COMPUTER & TECH. L.J. 491, 504 (1995).

[151] United States v. Motto, 70 F. Supp. 2d 570, 572 (E.D. Pa. 1999).

[152] *Id.* at 572-73 n.2.

[153] *Id.*

> presence of a business whose work is considerably more chaste than that of Paulino Reage or the Marquis De Sade. AOL's role, if any, as 'enabler' is therefore of no sentencing moment.[154]

Finally, cyberstalking does not just involve a man stalking a woman in a state of obsession. Cyberstalking has opened the door for stalkers to use the Internet to intimidate their victims by *using* the services provided through the Internet. For example, one cyberstalker terrorized Skip Press, an author whose works are sold by Amazon.com, by posting nasty messages on Amazon's comment page about Press' book.[155] This cyberstalker sent Press e-mail messages alleging that the Attorney General of Washington was investigating Press for posting these bogus reviews himself.[156] Press now has a web site detailing his struggles with the ISPs and content providers to remove the incorrect comments:

> Amazon.com did not respond to my e-mail of explanation. Instead, it made things worse, pulling down all the positive reviews that came in from my friends, taking down my Author Comments, and leaving the bogus bad 'reviews' up for all to see . . . . I called its legal department.
>
> I also made phone calls to America Online public relations (some of the nasty posts originated from AOL, it seemed), Earthlink, and other places. I got quick results, using the phone: Earthlink (my ISP) was its usual Johnny-on-the-spot about handling abuses to customers. A technical specialist researched it and assured me the 'troll' was not originating on Earthlink, even though he made it appear that way.
>
> AOL PR people told me that I was not a subscriber, and therefore it could not offer much assistance. If I wanted information about any AOL member, I would have to subpoena AOL. (This is why there are newsgroups like aol.sucks.)[157]

Press ends his web site with a warning: "If you get cyberstalked, you'll need cunning, real-life solutions, and friends to combat it. Just don't expect the authorities to rush to your aid; they have too much else to do. For that to change, someone will probably have to die at the hands of a cyberstalker."[158]

---

[154] *Id.* at 579.

[155] Skip Press, *Fighting Cyberstalking,* COMPUTEREDGE ONLINE, *at* http://members.tripod.com/cyberstalked/skippress.htm (last visited Nov. 11, 2000).

[156] *See id.*

[157] *Id.*

[158] *Id.*

Stalking is not the only crime that happens in cyberspace. For example, an "online system can be used in the planning or execution of almost any imaginable crime: drug dealing; pornography operations; robberies and burglaries; illegal transfer of inside information on stocks; bribery and graft; gambling; fraud; embezzlement; violating export regulations; the list goes on and on."[159] However, many of these crimes, especially stalking, traditionally require evidence of intent to commit the crime.[160] In the context of a cyberstalking situation, does the knowledge of the material really matter if the ISP does not intend for the victim to be fearful? Without the intent to injure or harass elements required by stalking, there simply is no crime. Therefore, an ISP should not be held criminally liable for the actions of its subscriber, unless it clearly knows about the stalking activity and allows it continue.

V. CONCLUSION

The Internet is not only a new medium; it is a new frontier. The advantages of this new communication medium are numerous. Now, people can express themselves in ways unimaginable just decades ago. This technology is the first step toward truly anonymous communication. The practical effects of freedom of speech, freedom of association and freedom from the body have never been so accessible.

The new freedoms afforded by the Internet also bring risks of abuse. The Internet has offered sick-minded people a new arena to prey on innocent victims. Therefore, the anti-stalking laws should be adapted to provide victims a means for fighting this dangerous and senseless activity on the Internet. Specifically, the requirement of a credible threat should be eliminated from current anti-stalking laws.

However, there seems to be no reason why an ISP should incur liability for activities of its subscribers, unless the ISP actually knows that the crime is being committed. The ISP should not be held liable if someone decides to abuse access to the Internet. Cyberstalkers like Dellapenta and Jake Baker alone are to blame and they alone should be punished for their crimes.

---

[159] LANCE ROSE, NETLAW: YOUR RIGHTS IN THE ONLINE WORLD 202 (1995).

[160] *See, e.g.*, CAL. PENAL CODE § 646.9 (West 1999 & Supp. 2000) ("Any person who willfully, maliciously, and repeatedly follows or harasses another person and who makes a credible threat *with the intent* to place that person in reasonable fear for his or her safety, or the safety of his or her immediate family, is guilty of the crime of stalking.") (emphasis added).