Cyberstalking, a New Crime: Evaluating the Effectiveness of Current State and Federal Laws

Naomi Harlin Goodno

Follow this and additional works at: http://scholarship.law.missouri.edu/mlr

Part of the Law Commons

Recommended Citation
Available at: http://scholarship.law.missouri.edu/mlr/vol72/iss1/7

This Article is brought to you for free and open access by the Law Journals at University of Missouri School of Law Scholarship Repository. It has been accepted for inclusion in Missouri Law Review by an authorized administrator of University of Missouri School of Law Scholarship Repository.
Cyberstalking, a New Crime: Evaluating the Effectiveness of Current State and Federal Laws

Naomi Harlin Goodno*

I. INTRODUCTION

The Internet is a powerful and wonderful tool that has ushered in a new information age. If purposely misused, however, the internet can be terrifying, and even deadly. Imagine a distressed woman discovering the following messages on the Internet that was falsely attributed to her:

"Female International Author, no limits to imagination and fantasies, prefers group macho/sadistic interaction . . . stop by my house at [current address]. Will take your calls day or night at [current telephone number]. I promise you everything you've ever dreamt about. Serious responses only."¹

Or, imagine the fear generated by the following e-mail messages sent over and over again from someone who remained anonymous, but seemed to have specific knowledge of the recipient’s personal life:

"I'm your worst nightmare. Your troubles are just beginning."²

Or, imagine the terror experienced by a woman who discovers a website with the following message and realizes that she is the "her":

"Oh great, now I'm really depressed, hmmm . . . looks like it's suicide for me. Car accident? Wrists? A few days later I think, 'hey, why don't I kill her, too? =)."³

². Id. at 23.
³. Id. at 112 (omission in original).

* Assistant Professor of Law, Pepperdine University School of Law; A.B., 1995, Princeton University; J.D., 1999, University of California, Berkeley, Boalt Hall School of Law; 1999-98, studied at Harvard Law School. The author thanks Dean of Research and Professor Richard Cupp for his comments, Professor Ruth Gordon and Professor Marci Peaks for their encouragement and advice, and Kelly Sinner, Dan Himebaugh and Christiana Sambor for their research and editing assistance.
All of these messages are examples of cyberstalking. Generally defined, stalking involves repeated harassing or threatening behavior.\(^4\) Today, advances in technology have created a new crime: cyberstalking.\(^5\) While there is not a universally accepted definition, cyberstalking involves the use of the Internet, e-mail, or other means of electronic communication to stalk or harass another individual.\(^6\) The use of electronic technology has broadened the ways stalkers can harass their victims.

This is a real problem. A 1999 Report from the Department of Justice suggests there might be tens of thousands of cyberstalking incidents each year.\(^7\) For example, the Department of Justice reported that in Los Angeles twenty percent of the 600 stalking cases were classified as cyberstalking; while in New York, over forty percent of the stalking cases were classified as cyberstalking.\(^8\) "The link between cyberstalking and the sexual abuse of children is also recognized by the U.S. government."\(^9\)

This article explores how the nature of cyberstalking represents a form of behavior distinct from "offline stalking."\(^10\) As such, the interpretation of many of the statutes dealing with offline stalking may be inadequate to ad-

\(^4\) U.S. Department of Justice, Stalking and Domestic Violence: Report to Congress 1 (May 2001), available at http://www.ncjrs.org/pdffiles1/ojp/186157.pdf [hereinafter Report to Congress]. Stalking behavior includes, but is not limited to following a person, appearing at a person's home or business, harassing communications and/or messages (e.g., phone calls, letters), or vandalizing property. Id.


Stalking generally refers to 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. These actions may or may not be accompanied by a credible threat of serious harm, and they may or may not be precursors to an assault or murder. Id. With cyber-harassment, the purpose remains the same: to cause distress to the targeted individual and to derive power from that distress.

\(^7\) Report to Congress, supra note 4, at 3-4.

\(^8\) Id. at 4.


\(^10\) For purposes of this article, "offline stalking" refers to stalking that occurs without communication via the computer. "Cyberstalking" or "online stalking" refers to stalking that occurs via the computer with the use of the Internet and e-mail.
dress the problem.\(^\text{11}\) The first part of this article explores the differences between offline stalking and cyberstalking. The second part examines what the criminal elements of cyberstalking should be in light of these differences. The third part considers how these differences create gaps in both state and federal stalking statutes so that it may be difficult to adequately prosecute all aspects of cyberstalking. This section also suggests ways to close these gaps. The fourth part deals with potential issues in criminalizing cyberstalking and how these issues might be resolved. Finally, the Appendix to the article sets forth all state and federal stalking laws and how they might currently deal with cyberstalking, if at all.\(^\text{12}\)

II. CYBERSTALKING VS. OFFLINE STALKING

A. Brief Review of Offline Stalking

While cyberstalking is as recent a phenomena as the Internet itself, even offline stalking is a relatively new crime. Generally, the goal of a stalker is to exert "control" over the victim by instilling fear in her; and often such conduct leads to physical action.\(^\text{13}\) California enacted the first stalking statute (targeted at offline stalking) in 1990 in response to the murder of Rebecca Schaeffer, star of the television series *My Sister Sam*.\(^\text{14}\) Schaeffer was helpless in stopping an obsessed fan who had stalked her for over two years. The stalking escalated and the fan eventually attacked and murdered her.\(^\text{15}\)

\(^\text{11}\) Law enforcement has often not caught up with the times, and officials are in many cases simply telling the victims to avoid the websites where they are being harassed or having their privacy violated. Some assistance can be found by contacting the web host companies (if the material is on a website) or the ISP of the abuser. Many victims note that persistence is key. At times the seriousness of the impact of this type of violation is not comprehended and the third party facilitators of cyberstalkers tell the victim to work it out with their harasser.

\(^\text{12}\) This article is limited to exploring cyberstalking in the criminal context. There is a host of other legal issues, particularly in the civil realm, which is beyond the scope of this article. See, e.g., Joanna Lee Mishler, *Cyberstalking: Can Communication via the Internet Constitute a Credible Threat, and Should an Internet Service Provider Be Liable if It Does?*, 17 SANTA CLARA COMPUTER \& HIGH TECH. L.J. 115 (2000) (addressing the issue of vicarious liability for Internet Service Providers in cyberstalking cases). In a later article, I intend to explore potential civil remedies for cyberstalking.

\(^\text{13}\) See id. at 120-25.

\(^\text{14}\) 2 WAYNE R. LAFAVE, SUBSTANTIVE CRIMINAL LAW § 16.4(b), at 575 (2d ed. 2003).

\(^\text{15}\) Id.
Other states, and soon the federal government, followed California's lead and enacted stalking statutes to "fill gaps in the law."\(^{16}\) Legislatures recognized the need to stop stalkers before the stalking developed "into a more serious threat to a victim's personal safety."\(^{17}\) Additionally, stalking laws were enacted "to eliminate behaviors which disrupt normal life for the victim, and to prevent such behaviors from escalating into violence."\(^{18}\) Statutes dealing with offline stalking were both preventative and proactive because they were "intended to criminalize certain acts of harassment in order to prevent more serious violent conduct by the stalker."\(^{19}\)

Despite the enactment of these laws, offline stalking is still a major problem. In this country alone, almost half a million victims are stalked each year, and approximately eighty-five percent are ordinary people without any celebrity or public status.\(^{20}\) Offline stalking has "a profound effect upon the victim" by causing post-traumatic stress disorder, depression and serious emotional distress, and also by escalating to physical attacks.\(^{21}\) While the goal — to control and intimidate — is similar in both offline stalking and cyberstalking cases, there are differences in how the cyberstalker achieves this goal. These differences create legal problems for victims of cyberstalking.

B. Differences Between Cyberstalking and Offline Stalking

Some experts believe that cyberstalking is synonymous with traditional offline stalking because of the similarities in content and intent.\(^{22}\) Similarities that are pointed to include: a desire to exert control over the victim;\(^{23}\) and, much like offline stalking, cyberstalking involves repeated harassing or threatening behavior, which is often a prelude to more serious behavior.\(^{24}\) While these similarities do exist, cyberstalking differs from offline stalking in five important ways. These five differences are crucial because they are the reasons why traditional stalking statutes may fall short of addressing cyberstalking.

1. **Cyberstalkers can use the Internet to instantly harass their victims with wide dissemination.** Cyberstalking takes place over the Internet.

\[^{17}\text{Id. at 743.}\]
\[^{18}\text{James Thomas Tucker, Stalking the Problems With Stalking Laws: The Effectiveness of Florida Statutes Section 784.048, 45 FLA. L. REV. 609, 617 (1993).}\]
\[^{19}\text{Id. Cyberstalking statutes should reflect the same goals of being proactive and preventative.}\]
\[^{20}\text{2 LAFAVE, supra note 14, § 16.4(a), at 574.}\]
\[^{21}\text{Id.}\]
\[^{22}\text{Servance, supra note 5, at 1219.}\]
\[^{23}\text{REPORT TO CONGRESS, supra note 4, at 1.}\]
\[^{24}\text{REPORT TO CONGRESS, supra note 4, at 1; Harry Valetk, Mastering the Dark Arts of Cyberspace: A Quest for Sound Internet Safety Policies, 2004 STAN. TECHNICAL L. REV. 2, 54 (2004).}\]
While obvious, this distinction is extremely important because the Internet is a borderless medium that allows instantaneous and anonymous distribution of one's message. In this cyber-age, websites, e-mail, chat rooms, anonymous electronic bulletin boards, instant messaging, and other web communication devices allow cyberstalkers to quickly disseminate intimidating and threatening messages. Moreover, Internet content can be widely distributed to a larger, more public forum than any conventional form of offline stalking and it can be done so inexpensively and efficiently.

For example, an offline stalker may harass the victim by repeatedly telephoning the victim. However, every telephone call is a single event that requires the stalker's action and time. This behavior can easily snowball online because, with only one action, the stalker can create a harassing e-mail message that the computer systematically and repeatedly sends to the victim thousands upon thousands of times (e.g., an “e-mail bomb”).

Moreover, cyberstalkers can create a website where they post harassing and threatening statements. Thus, instead of sending harassing letters, the cyberstalker has the ability to post threatening comments for the whole world to view. Such websites allow for constant harassment, which compounds the invasion of privacy and ultimately the impact of cyberstalking.

2. Cyberstalkers can be physically far removed from their victim. Offline stalking often entails situations where the stalker is physically near the victim. Cyberstalkers, however, can use the Internet to terrify their victims no matter where they are; thus, they simply cannot escape. The seemingly unlimited reach of the Internet makes cyberstalking distinct from offline stalking in three ways.

First, it provides cyberstalkers a cheap and easy way to continue to contact their victim from anywhere in the world. Cyberstalkers can stalk their victims from a different city, state, or even country, so long as there is access to the Internet, a medium which is likely cheaper than a telephone and faster than mail. Second, there is a sinister element to the secrecy of the cyberstalker's location. The uncertainty of the cyberstalker's location can leave the victim in a state of constant panic as she is left wondering whether her stalker is in a neighboring house or a neighboring state. Finally, the physical location of the cyberstalker can create several jurisdictional problems. Because cyberstalking can easily take place across state lines, state prosecutors may confront jurisdictional problems in enforcing any state laws. To name just a few of these jurisdictional problems, issues arise as whether the applicable state law is from the state where the stalker is located or from the state where the victim lives. From a practical standpoint, it makes the prosecution of cy-

25. BOCU, supra note 9, at 2.
26. HITCHCOCK, supra note 1, at 100-16.
27. REPORT TO CONGRESS, supra note 4, at 3; Valetk, supra note 24, at 54.
berstalking even more difficult because it may require collecting evidence from many jurisdictions.  

3. **Cyberstalkers can remain nearly anonymous.** There is a common misperception that cyberstalking is less dangerous than offline stalking because it does not involve physical contact. However, the opposite is true. While a potential stalker may be unwilling to personally confront the victim, the anonymity of the Internet allows individuals, who may not otherwise engage in offline stalking, to send harassing or threatening electronic communication.

The environment of cyberspace allows individuals to overcome personal inhibitions. The ability to send anonymous harassing or threatening communications allows a perpetrator to overcome any hesitation, unwillingness, or inabilities he may encounter when confronting a victim in person. Perpetra-

29. Some state and local law enforcement agencies also have been frustrated by jurisdictional limitations. In many instances, the cyberstalker may be located in a different city or state than the victim making it more difficult (and, in some cases, all but impossible) for the local authority to investigate the incident. Even if a law enforcement agency is willing to pursue a case across state lines, it may be difficult to obtain assistance from out-of-state agencies when the conduct is limited to harassing e-mail messages and no actual violence has occurred. A number of matters have been referred to the FBI and/or U.S. Attorney's offices because the victim and suspect were located in different states and the local agency was not able to pursue the investigation.


30. The issue of whether anonymity should be regulated on the Internet is a current debate. See, e.g., George F. du Pont, The Criminalization of True Anonymity in Cyberspace, 7 MICH. TELECOMM. & TECH. L. REV. 191, 196-216 (2000-2001). Du Pont's analysis distinguishes between "true anonymity," which is untraceable, and "pseudo-anonymity," which, although indirectly, is inherently traceable. Id. at 196. He cites a historical precedent for pseudo-anonymity, and realizes its social good for anonymous public debate (i.e., the American Revolutionary period, The Federalist Papers, modern political campaigns, etc.). Id. Where the courts and history have recognized a free speech value to anonymity, it has almost always meant pseudo-anonymity. Id. But true anonymity is prone to abuse and danger. Cyberspace has greatly increased the ease with which true anonymity can be attained. Du Pont's proposal is to criminalize all non-privileged, truly anonymous communication in cyberspace and mandate that all anonymous communication in cyberspace be merely pseudo-anonymous. See id. at 196-216.


32. See BOCU, supra note 9, at 90-106.
tors may even be encouraged to continue these acts. Additionally, the anonymity of the Internet allows cyberstalkers to follow and spy on their victims in cyberspace for extended periods of time without the victim’s knowledge.

As one scholar has explained, there is a “veil of anonymity” on the Internet that puts cyberstalkers “at an advantage.” Anonymity makes it difficult to identify, locate, and arrest stalkers. In fact, cyberstalkers can use technologies to strip away many identifying markers from their communications.

4. Cyberstalkers can easily impersonate the victim. Unlike offline stalking, the cyberstalker can easily take on the identity of the victim and create havoc online. While pretending to be the victim, the cyberstalker can send lewd e-mails, post inflammatory messages on multiple bulletin boards, and offend hundreds of chat room participants. The victim is then banned from bulletin boards, accused of improper conduct, and flooded with threatening messages from those the stalker offended in the victim’s name.

This is exactly what happened to Jane Hitchcock, who was cyberstalked by the owner of a company after she complained about the company’s services. Intending to provoke others, the cyberstalker impersonated Hitchcock and posted inflammatory comments on Web pages and sent e-mails in her name aimed at provoking others to “flame” her. Moreover, for over a year, the cyberstalker “e-mail bomb[ed]” her by sending thousands of harassing messages to her e-mail account. He would also send thousands of harassing messages to her husband’s and her employer’s e-mail accounts, sometime impersonating Hitchcock, which eventually flooded the accounts rendering them “useless.” The cyberstalker’s actions became so unbearable that Hitchcock was forced to physically move, but that did not stop him. He eventually found her online and would begin to harass her again. Hitchcock sued him, but the cyberstalker was never held criminally liable.

33. REPORT TO CONGRESS, supra note 4, at 2.
34. Such conduct would still be considered harassment if the cyberstalker has the intent to harass the victim. See 1999 REPORT ON CYBERSTALKING, supra note 29, at 12.
36. Id. at 1388.
37. For example, impersonating Hitchcock, the cyberstalker sent the following e-mail to her employer: “I’m an assistant teacher at UMUC and I think you and the whole of UMUC are a bunch of morons insidiously festering away your small brains. I may or may not resign. I may stay to awaken you idiots.” HITCHCOCK, supra note 1, at 8.
38. Id.
39. Id. See also BOCU, supra note 9, at 2.
40. Hitchcock sued her cyberstalker who eventually settled. BOCU, supra note 9, at 2-3. The cyberstalker also pled guilty to conspiracy to commit mail fraud and per-
5. Cyberstalkers can encourage “innocent” third-party harassment. Perhaps most frightening, and unique to cyberstalking, is that cyberstalkers can incite other “innocent” third parties to do their stalking for them. For example, in California, a fifty-year-old defendant used the Internet to solicit the rape of a twenty-eight-year-old woman who had rejected the defendant’s romantic advances. The defendant then terrorized her by impersonating her in various Internet chat rooms and posting her telephone number, address, and messages that she fantasized of being raped. Because of these messages, on separate occasions, at least six men knocked on the woman’s door saying that they wanted to rape her. Hitchcock experienced a similar form of cyberstalking when her cyberstalker advertised her telephone and address in an alt.sex newsgroup advertising for “sadistic interaction.”

Another example of duping “innocent” third parties to do the harassing involved a cyberstalker who sent hate e-mail in his victim’s name, often with her telephone number and address, “to groups of Satanist, drug users and pornographers.” She only discovered this when the cyberstalker’s actions prompted a threatening and terrifying telephone call from a man who lived twenty minutes from her: “[y]ou’d better get a gun because the next time we read about you it will be in a police report.” It was later discovered that the cyberstalker was the victim’s disgruntled business acquaintance, but the victim had no criminal recourse.

In many ways, the Internet makes many of the frightening characteristics of offline stalking even more intense. It provides cyberstalkers with twenty-four-hour access, instantaneous connection, efficient and repetitious action, and anonymity. On top of all that, cyberstalkers can easily pretend that they are different people. The possibilities open to cyberstalkers are as endless as the borders of the ubiquitous Internet. It is for these reasons that the laws should be updated to deal with this new crime.

jury for the conduct related to Hitchcock’s original complaints. Id. at 2. However, he was never prosecuted for any crime related to stalking or harassment.

41. Other scholars have referred to this as “stalking by-proxy.” See id. at 25-26.

42. See Bill Wallace, Stalkers Find a New Tool — The Internet E-mail is Increasingly Used to Threaten and Harass, Authorities Say, SAN FRANCISCO CHRON., Jul. 10, 2000, available at http://www.sfgate.com/cgi-bin/article.cgi?file=/chronicle/archive/2000/07/10/MN39633.DTL.

43. See id.

44. Hitchcock, supra note 1, at 11.


46. Id.

47. Id.

48. See, e.g., Radosevich, supra note 35, at 1389. (“Until broader language is implemented to cover the use of new information technologies and methodologies in [cyber]stalking cases, victims may have to search for alternative solutions.”). Some of those solutions include: utilizing more computer specialists on law enforcement task
III. EXAMINING THE CRIMINAL ELEMENTS OF CYBERSTALKING

Since there are differences between cyberstalking and offline stalking, the question arises whether the current stalking laws, which were drafted to criminalize offline stalking, are adequate to deal with all aspects of cyberstalking. The answer: not fully. Therefore, the remainder of this article sets forth what the elements of cyberstalking should be in order to adequately deal with the crime.

The Appendix to this article summarizes the current stalking laws in all fifty states and the federal equivalents. The Appendix sets forth whether the statute specifically addresses cyberstalking and, if not, how the existing stalking statute might be used to prosecute cyberstalking crimes. Those statutes that have attempted to incorporate cyberstalking into their offline stalking statutes are often inadequate because of the differences between cyberstalking and offline stalking. Indeed, even some of the statutes that were enacted to target cyberstalking still fail to address all of its vices. To understand these inadequacies, the general elements of offline stalking need to be considered in comparison to what the elements should be for this new crime of cyberstalking.

As set forth in this next section, cyberstalking and offline stalking should share the same intentional mental state requirement; but to be effective, cyberstalking statutes should criminalize conduct that either puts a “reasonable person” in fear of bodily harm or causes severe emotional distress. Furthermore, the cyberstalking statute should specifically address situations where the cyberstalker entices third parties to harass for them.

a. The “intentional” mens rea requirement. As with most crimes, offline stalking has both mens rea and actus reus requirements. Generally, a stalker must “willfully or intentionally” (mental state) engage in “repetitive conduct” or a “course of conduct” (actus reus) that causes the victim to fear, or that the stalker should have known would cause the victim to fear for her safety. Although there are many differences in offline stalking statutes, the majority of them have a similar intentional mental state requirement.
As far as cyberstalking is concerned, this “intentional” mental state requirement is appropriate. The point of cyberstalking laws, much like offline stalking statutes, should be to stop individuals from purposefully causing another to fear. Like an offline stalker, a cyberstalker should have to “intentionally” engage in conduct that causes his target to fear for her safety (or should have known would cause fear for her safety).

b. The need to criminalize a “course of conduct” that would cause a “reasonable person” to fear for her safety. A more difficult analysis arises concerning the actus reus requirement. What “conduct” should be criminal? There are two considerations here. First, most offline stalking statutes require the conduct be “repetitive.” In other words, to be in violation of the law, the stalker has to engage in conduct at least more than once in such a way that causes the victim to fear. This requirement is suitably applicable to cyberstalking. It is appropriate to require that the cyberstalker engage in “repeated” conduct; e.g., e-mailing a harassing message more than once; or posting a message on a website that causes others to harass the victim more than once. A lesser requirement would not only undercut the definition of a “course” of conduct, which implies that there must be ongoing acts, but it would also trivialize the seriousness of a continuous pattern of harassment. Moreover, punishing merely one instance of harassing conduct may unjustly penalize one who acts once out of anger, verses one who engages in a series of terrifying acts.

The second consideration is where the real issue arises when offline stalking laws are applied to cyberstalking. This second matter concerns the type of conduct that is criminal. Generally, there are three different types of conduct that offline stalking statutes criminalize: (1) conduct requiring an

53. See infra Appendix.
54. See id.
55. See, e.g., ARK. CODE ANN. § 5-71-229(d)(1)(a) (2006) (defining course of conduct as conduct composed of two or more acts separated by at least thirty-six hours, but occurring within one year); see also infra Appendix.
56. It is difficult to attempt to categorize all stalking statutes because there is a huge variety in defining what conduct constitutes “stalking.” See, e.g., Keirsten L. Walsh, Comment, Safe and Sound at Last? Federalized Anti-Stalking Legislation in the United States and Canada, 14 DICK. J. INT'L L. 373 (1996). For purposes of this article, the laws have been generally divided into three categories to illustrate what elements best define cyberstalking; however, not all stalking laws necessarily distinctly fit into one of the three categories.
element of physical or visible proximity to the victim;\textsuperscript{57} (2) conduct conveying verbal or written threats or threats implied by conduct, \textit{i.e.}, a "credible threat";\textsuperscript{58} and (3) conduct that would cause a "reasonable person" to fear physical harm or to suffer severe emotional distress (hereinafter the "reasonable person standard").\textsuperscript{59} As set forth below, statutes in categories one or two fall far short in combating cyberstalking because such statutes focus solely on the perpetrator's conduct. On the other hand, laws with a "reasonable person" standard can fully address cyberstalking because such laws correctly focus on the effect of the perpetrator's conduct on the victim (\textit{e.g.}, the fear felt by the victim).\textsuperscript{60}

\textbf{(i) Problems with physical proximity requirement.} Currently, there are only a few offline stalking statutes that require that the defendant engage in conduct that has some requirement of actual physical pursuit.\textsuperscript{61} Since the very nature of cyberstalking allows the cyberstalker to be hundreds or thousands of miles away from his victim, statutes that require an element of physical or visual proximity cannot address the crime.

For example, in one 1996 cyberstalking case in Georgia, a cyberstalker posted a crude message on a website that gave his victim's telephone number and home address and advertised that she was a prostitute. Many responded to the message by calling and showing up at her front door and "innocently" harassed the victim.\textsuperscript{62} Under Georgia's stalking statute at that time (the statute has since been amended),\textsuperscript{63} the cyberstalker was found innocent of stalking because his conduct did not include the physical pursuit of the victim.\textsuperscript{64}

\textbf{(ii) Problems with credible threat requirement.} Many current stalking statutes require the perpetrator to make a "credible threat" of violence against the victim.\textsuperscript{65} Generally, a credible threat is "a verbal or written threat" cou-

\textsuperscript{57} ARIZ. REV. STAT. ANN. § 13-2923 (2001).
\textsuperscript{58} See, e.g., ALASKA STAT. § 11.61.120(a)(4) (2006); see also infra Appendix.
\textsuperscript{59} See, e.g., ARIZ. REV. STAT. ANN. § 13-2921(E) (2001); CAL. PENAL CODE § 646.9(g) (1999); CONN. GEN. STAT. § 53a-181e (2001); IDAHO CODE ANN. §§ 18-7905 to -7906 (2004); MINN. STAT. § 609.749 (2003 & Supp. 2006); see also infra Appendix.
\textsuperscript{61} See, e.g., CONN. GEN. STAT. § 53a-181d (2001); IOWA CODE § 708.11(1)(b) (2003); MD. CODE ANN., CRIM. LAW § 3-802(a) (West 2002 & Supp. 2003); N.J. STAT. ANN. § 2C:12-10(1) (West 2005); N.C. GEN. STAT. § 14-277.3(a), (c) (2003); UTAH CODE ANN. § 76-5-106.5(1)(a) (2003); WYO. STAT. ANN. § 6-2-506 (2005); see also infra Appendix.
\textsuperscript{63} See GA. CODE ANN. § 46-5-21 (2004).
\textsuperscript{64} See Cyberstalked: Our Story, supra note 62.
\textsuperscript{65} Over one-third of state stalking statutes have a credible threat requirement. See infra Appendix; see also REPORT TO CONGRESS, supra note 4, at 7.
pled “with the apparent ability to carry out the threat” so as to cause the victim fear. It is the requirement of the “threat” and the “apparent ability” to carry it out that makes this standard inadequate to deal with cyberstalking in at least four ways.

First, the requirement that there be an overt “threat” is problematic. Such a requirement leaves a gap for conduct that does not specifically threaten, but would still cause a reasonable person to fear for her safety. Stalkers typically do not explicitly threaten their victims, but instead “pursue a course of conduct that, when taken in the aggregate, would cause fear in a reasonable person but stops short of [a] . . . threat.”

For example, an offline stalker may lurk behind bushes to watch the victim, follow her, continuously call her and hang-up, and send black roses to her. Since none of these actions include an overt threat, such punishment would likely not establish the credible threat requirement. In cyberstalking cases, a statute with a credible threat requirement does not protect against electronic communications (such as thousands of e-mail messages) that are harassing, but do not include an actual threat.

These issues associated with a credible threat standard are being litigated in offline stalking cases. One state replaced the credible threat requirement in its stalking statute with a reasonable person standard because of these issues, which become even more acute in cyberstalking cases. In Iowa v. Limbrecht, the court recognized the change in the statute and explained that whether a stalking conviction would be reversed depended on which standard applied. The Limbrecht defendant, a prison inmate became obsessed with a young woman, Stacy Corey, who worked as an employee at the prison. The defendant’s repetitive, intimidating stares and lies to other inmates about how he had sexual relations with her forced Corey to quit and move. However, the defendant’s obsession continued when he was released from prison. He found Corey’s new address and sent vulgar, untrue letters to Corey’s husband about how Corey had sexual relations with many inmates when she worked at the prison. The defendant also drove by Corey’s house a number of times, which ultimately led to his arrest and stalking conviction. The defendant appealed his conviction arguing that he never explicitly threatened to hurt Corey, the court acknowledged that the defendant never threatened Corey,

66. CAL. PENAL CODE § 646.9(g) (West 1999) (emphasis added).
67. Merschman, supra note 60, at 267.
68. See, e.g., CAL. PENAL CODE § 646.9 (harassing electronic communications do not constitute cyberstalking unless there is a credible threat); Iowa v. Limbrecht, 600 N.W.2d 316, 319 (Iowa 1999); United States v. Alkabazah, 104 F.3d 1492, 1494-95 (6th Cir. 1997).
70. 600 N.W.2d at 316-19.
71. Id. at 317.
72. Id. at 318.
73. Id. at 318-19.
but rejected his argument because it "harken[ed] back" to the former version of the stalking statute which required proof of a "credible threat" against another person. Under the amended version of the statute which adopted the reasonable person standard, the court found that the defendant's actions assumed frightening proportions and was no less threatening than an actual threat.

As exemplified by Limbrecht, the issue of whether a credible threat requirement is the appropriate standard is being debated in offline stalking cases. This issue, however, is even more acute with cyberstalking. The Internet makes it easier for a cyberstalker to engage in a threatening course of conduct in a much shorter period of time than an offline stalker. In Limbrecht, the stalker sent two letters over the course of one month. Cyberstalkers, on the other hand, can easily use the Internet to send hundreds, even thousands, of frightening e-mail messages — similar to the letters sent in Limbrecht — in a matter of one hour, which over days and weeks can create havoc for a victim. If there is not one explicit threat in any of those thousands of e-mail messages, then the victim cannot establish the credible threat requirement.

74. Id. at 1319. See also IOWA CODE ANN. § 708.11(1)(b)(1) (2003) (defining a "credible threat" as "a threat made with the intent to place a reasonable person in like circumstances in fear of death or bodily injury, coupled with the apparent ability to carry out the threat.").

75. Limbrecht, 600 N.W.2d at 319 (citing IOWA CODE § 708.11(1)(b) (1997)). See also 1994 IOWA ACts 1093, § 4.

76. When determining whether to adopt a credible threat requirement or reasonable person standard, the drafters of the federal model rule specifically choose to use the reasonable person standard instead of the credible threat requirement. See Walsh, supra note 56, at 389 ("On the other hand, the model code did not use the language 'credible threat' when defining the behavior directed toward the victim. In order to prohibit behavior in the form of threats implied by conduct, the model code purposely omitted this language for fear it would be construed as requiring an actual verbal or written threat.").

77. REPORT TO CONGRESS, supra note 4, at 45 n.3. See also Federal Interstate Stalking Statute, 18 U.S.C. § 2261A(1) (2006) (codifying a "reasonable fear" standard).

78. Limbrecht, 600 N.W.2d at 317-18.

79. For example, a cyberstalker can send "e-mail bombs" — meaning that the cyberstalker can generate one e-mail message and use the computer to continuously send the same message over-and-over to the same recipient.

80. The overt threat also usually has to be verbal or written, which may also raise issues in cyberstalking cases. A "verbal" threat requires physical nearness to the victim, which, analogous to statutes that have a "physical proximity" requirement, unnecessarily carves out many cyberstalking cases since the stalking takes place virtually. A "written" threat requirement seems more applicable to cyberstalking, but even that may be problematic. If the statute has a written threat requirement, but does not make clear that "written" includes "electronic communication," then some computer generated messages may not be included. Many statutes do not cover the various types of electronic communications (e.g., e-mail, message boards, chat rooms, blogs,
A second problem with a credible threat requirement in cyberstalking cases is an issue of receipt. A “threat” suggests a communication directly from the stalker to the victim. But a cyberstalker can easily post terrifying messages without ever being in direct contact with the victim or without the victim ever personally receiving the message. A cyberstalker can broadcast harassing messages to the entire Internet world by posting them on websites and blogs. In cyberstalking cases then, the stalker can quickly and effortlessly engage in terrifying conduct to harass the victim — conduct no less disturbing than an actual threat — with world-wide dissemination.

For example, in one case a cyberstalker created a webpage “dedicated” to his young victim, Amy Boyer. The cyberstalker was a fellow student who, unbeknownst to Boyer, wrote detailed fantasies about Boyer and messages about Boyer’s daily life — such as what she wore on any particular day, where she went, what she was doing — and posted them on the webpage. These postings went on for about two years and tragically ended when the stalker murdered Boyer and committed suicide. Neither Boyer nor her family was aware of any of these messages on the website until after she was murdered. Although this case was never litigated, it would likely have been difficult for Boyer to establish that there was a credible threat because a threat was never sent directly to her.

A third problem that the credible threat requirement creates in cyberstalking cases is that it requires the victim to prove that the cyberstalker had the “apparent ability” to carry out whatever he threatens. What if the cyberstalker sends a threatening e-mail to the victim from across the country? It would seem that the victim might then have the burden to prove that the cyberstalker had the financial ability to buy a plane ticket to travel across the country to carry-out that threat. Such a requirement is onerous and unnecessary, particularly since the victim may not even know the true identity or location of the cyberstalker.

In fact, the victim may not even know where an anonymous cyberstalker is physically located. For all she knows the cyberstalker might be next door, at her workplace, or across the country, making it even more difficult to establish that a threat could be carried out. The Internet allows for anonymity when sending any type of electronic communication. Cyberstalkers covet anonymity because it allows them to hide from reality and from their victims. Victims who are stalked by unknown persons cannot know the perpe-

81. HITCHCOCK, supra note 1, at 100-16.
82. Id.
83. See infra Part III (fully explaining United States v. Alkhabaz, 104 F.3d 1492 (6th Cir. 1997)).
84. See generally Rebecca K. Lee, Romantic and Electronic Stalking in a College Context, 4 WM. & MARY J. WOMEN & L. 373, 381-82 (1998). Also, because the
trator's habits or intentions. Thus, as their identities are concealed, so too are all the character traits of the perpetrators. Where the identities and abilities of cyberstalkers are unknown to the victim, it is impossible for the victim to determine whether the perpetrator has the apparent ability to carry out the threat. As a consequence, it will be extremely difficult, if not impossible, to show that an anonymous cyberstalker has the ability to carry out any threat.

The fourth problem with the credible threat requirement in cyberstalking cases is that it completely fails to address cases where the cyberstalker incites "innocent" third parties to harass the victim. In situations where, for example, the cyberstalkers take on the identity of the victim and post messages inviting gang rape, there is neither an overt threat, nor a threat sent from the cyberstalker directly to the victim.

In short, statutes which have a credible threat requirement — either those that have attempted to incorporate cyberstalking in preexisting statutes or those that have been specifically targeted at cyberstalking — cannot fully address all aspects of cyberstalking. This is because they focus on the cyberstalker's conduct. The reasonable person standard, however, is better in cyberstalking cases because it focuses on the fear that the cyberstalker intentionally meant to instill in his victim.

(iii) The reasonable person standard: the appropriate standard. Those stalking statutes that have a reasonable person standard provide the most successful way to prosecute cyberstalking. Such a standard has no physical proximity requirement. Furthermore, the standard addresses many of

Internet is "essentially a 'decontextualized' medium . . . people can send messages without revealing their handwriting or other clues to their personality . . . . Cyberstalkers can easily disguise themselves by adopting several false names and forging e-mail messages." Id. at 409. Furthermore, a victim may be more hesitant to report a threat if their stalker is anonymous. Id. at 382.

85. Id. at 382.
86. Rose Hunter, Cyberstalking (2001), http://gsulaw.gsu.edu/lawand/papers/fa01/hunter/ (discussing third party harassment under the Message Board section).
87. For purposes of this paper, the "reasonable person standard" is similar to statutes that criminalizes repeated conduct that "harasses," "annoys," or "alarms" (hereinafter "harassment statutes"). Some states have two statutes, one dealing with stalking and the other harassment. Often, the harassment statutes adopt the broad "to harass" standard. See, e.g., CONN. GEN. STAT. § 53a-182b (2001); N.D. CENT. CODE § 12.1-17-07 (1997); WASH. REV. CODE § 9.61.230 (2003). See also infra Appendix. The harassment standard may encompass many of the same cyberstalking situations that would be addressed by the reasonable person standard; however, as set forth in this section the best standard to apply to cyberstalking would be the reasonable standard. Moreover, many of the harassment statutes are limited to misdemeanors. See, e.g., ARK. CODE ANN. § 5-41-108(a)-(b) (2006); CAL. PENAL CODE § 653m (West 1999); CONN. GEN. STAT. § 53a-183 (2001); DEL. CODE ANN. tit. 11, §§ 1311-1312 (2001) (including the crime of "aggravated harassment" which is actually considered a class G felony); see also infra Appendix.
the problems created by statutes with a credible threat requirement. The reasonable person standard does not require that the cyberstalker send an explicit threat to the victim, nor does it require that the victim prove the cyberstalker had the ability to carry it out. Instead, the standard focuses on the victim and whether it is reasonable for her to fear for her safety because of the cyberstalker’s conduct.

Distinguishing between statutes that require a credible threat from those that use the “reasonable person” standard requires careful reading of the entire statute. The Delaware stalking statute, for example, makes it a crime for a person to “intentionally engage[] in a course of conduct directed at a specific person” that would cause “a reasonable person” fear.\textsuperscript{88} Facialy, this statute does not appear to require a credible threat. But, it is important to not immediately assume that this statute focuses only on the fear felt by the victim. Further reading reveals that “course of conduct” includes either maintaining physical proximity to the victim, conveying a verbal or written threat, or a threat implied by conduct (a standard akin to a “credible threat”).\textsuperscript{89} Thus, even though the “reasonable person” language appears in the statute, a full reading of it shows that it might be equivalent to all other cyberstalking statutes requiring a credible threat.

(iv) Criminalizing situations where the cyberstalkers entice “innocent” third-parties to harass. One of the most apparent differences between cyberstalking and stalking is that cyberstalkers can entice third parties to do the work for them.\textsuperscript{90} Currently, only Ohio has taken the approach to specifically criminalize such behavior.\textsuperscript{91} This is the best approach. So that neither cyberstalkers nor victims are unclear that this conduct is criminal, statutes criminalizing cyberstalking should directly provide that no person should use the Internet to cause another to engage in conduct that would cause a reasonable person to fear for her safety.

IV. CURRENT LAWS DEALING WITH CYBERSTALKING

A. Addressing the Gaps in State Laws

As illustrated in the Appendix to this article, state statutes that might be used to prosecute cyberstalking do not have clear and equal standards.\textsuperscript{92} Statutes with a physical proximity or a credible threat requirement are impractical and ineffective in prosecuting cyberstalkers. Statutes that are most useful and successful in prosecuting cyberstalkers and protecting victims are those

\textsuperscript{89} Id. See also IOWA CODE § 708.11(1)(b) (2003) (“Course of conduct” requires either repeatedly maintaining a visual or physical proximity, or a threat.).
\textsuperscript{90} See supra Part II.B.5.
\textsuperscript{91} OHIO REV. CODE ANN. § 2917.21(B) (LexisNexis 2006).
\textsuperscript{92} See infra Appendix.
which shift the focus from the perpetrator’s behavior to the effect on the victim.\textsuperscript{93}

Generally, there are three categories of state laws.\textsuperscript{94} The laws in each of these categories have gaps such that they may not fully be able to address all aspects of cyberstalking. Each of these categories is taken in turn.

1. State Statutes that Do Not Address Cyberstalking

First, there are some state laws that do not address cyberstalking at all. Most obvious are those statutes that have physical pursuit requirements.\textsuperscript{95} There are other statutes that do not address cyberstalking because it is unclear if they cover any form of electronic communication.\textsuperscript{96} For example, some states have a telephone harassment statute, but the statute only covers telephone communications, not specifically electronic communications.\textsuperscript{97} Laws that require physical pursuit and laws that fail to include electronic communications cannot reach cyberstalking.

2. State Statutes that May Address Some Aspects of Cyberstalking

The second general category of state statutes encompasses the majority of the current state laws. The laws in this category raise three issues.

First, some states have attempted to amend existing stalking statutes to cover cyberstalking via “electronic communications.”\textsuperscript{98} The type of electronic communications covered by these statutes varies. While some states simply inserted the general phrase “electronic communications” into existing statutes, others identified specific types of communications, e.g., e-mails, computer communications, or communications on the network.\textsuperscript{99} Although it is

\textsuperscript{93} Merschman, supra note 60, at 268-69.

\textsuperscript{94} As set forth in the Appendix to this article, the state stalking and harassment laws are literally all over the board. This section attempts to generally categorize them to show why some of the laws do not work in cyberstalking cases, and why others may work in part. The Appendix, however, provides a specific analysis for each state law. See infra Appendix.

\textsuperscript{95} See, e.g., CONN. GEN. STAT. § 53a-181 (2001); MD. CODE ANN., CRIM. LAW § 3-802 (West 2002 & Supp. 2005); IOWA CODE § 708.11 (2003); N.Y. PENAL LAW § 120.55 (McKinney 2004); N.Y. PENAL LAW § 120.60; see also infra Appendix.

\textsuperscript{96} See, e.g., ARK. CODE ANN. § 5-71-229 (2006); CONN. GEN. STAT. § 53a-181e (2001); D.C. CODE § 22-404 (2001); see also infra Appendix.

\textsuperscript{97} See, e.g., KAN. STAT. ANN. § 21-4113 (1995).

\textsuperscript{98} See, e.g., GA. CODE ANN. § 16-5-90 (2003) (“contact” means “any communication including without being limited to communication . . . by computer, by computer network, or by any other electronic device.”); HAW. REV. STAT. § 711-1106.5 (2003) (non-consensual contact includes contact via electronic mail transmission).

\textsuperscript{99} See, e.g., infra Appendix; CAL. PENAL CODE § 646.9(g)-(h) (West 1999) (including a computer within the meaning of an “electronic communication device,”
promising that some states are beginning to take notice of cyberstalking crimes, the results thus far have been a wide variety of mostly inadequate statutes with a hodgepodge of definitions, requirements, protections, and penalties.

Amending current stalking statutes to include electronic communications is a step in the right direction. Unfortunately, this is not enough. For example, New York's anti-stalking laws covers electronic communications, but state legislatures have introduced bills targeted specifically at cyberstalking and at making it a felony. This suggests that simply amending preexisting stalking statutes may be insufficient to combat cyberstalking.

Moreover, while some statutes may cover electronic communications, the language of the statutes seems to suggest that it would only apply to messages sent directly to the victim, e.g., an e-mail sent directly from the cyberstalker to his victim, but not to other Internet postings. Such statutes may unnecessarily carve out those cyberstalking cases like the Boyer case where the stalker created an entire website dedicated to following her every move, but never sent an e-mail directly to her. It also carves out those cases where the cyberstalker encourages "innocent" third party harassment.

and defining "electronic communications" according to 18 U.S.C. § 2510(12) (2006); HAW. REV. STAT. § 711-1106.5 (2003) ("Non-consensual contact" includes contact via electronic mail transmission); GA. CODE ANN. § 16-5-90 (2003) (including, but not limiting communication to communication by computer, computer network, or by any other electronic device); see generally Shawn Hutton & Sandy Haantz, Cyberstalking, National White Collar Crime Center, available at www.nw3c.org. The investigators and prosecutors of these units receive continual training in the fields of computer networks, surveillance, evidence gathering, as well as the proper resources to address these technical claims. Id.

100. N.Y. PENAL LAW § 240.30 (McKinney 1999 & Supp. 2001); N.Y. PENAL LAW § 120.45 (McKinney 2004).


102. Indeed, this change is necessary because, in many instances, New York felony stalking laws require that the perpetrator physically display a weapon or physically injure the victim. See, e.g., N.Y. PENAL LAW §§ 120.55(1), 120.60(1) (McKinney 2004). Such physical requirements carve-out cyberstalking cases.


104. HITCHCOCK, supra note 1, at 112.
This leads to the second issue. There is also a group of offline stalking statutes that have a credible threat requirement or the equivalent. There are many laws that require that the electronic communication between the cyberstalker and the victim include a specific threat, which is virtually the same as having a credible threat standard.\textsuperscript{105} Other statutes require that the communication contain a credible threat when the perpetrator is not physically pursuing the victim.\textsuperscript{106} And, there are even other statutes that, at first glance, seem to have a reasonable person standard, but upon close reading still require a credible threat.\textsuperscript{107} As set forth earlier in this article, a statute with a credible threat standard, even where electronic communications are included, cannot deal with all aspects of cyberstalking.\textsuperscript{108}

The final issue is that none of the statutes in this second category explicitly address situations where the cyberstalker dupes "innocent" third parties to harass his victim. For a few states, there may be a way to address this issue with the current laws, however, it has not yet been litigated. Some states have two types of general statutes that might address cyberstalking: those directed at stalking and those directed at harassment.\textsuperscript{109} Generally, harassment statutes have a broader reach addressing those situations where the stalker engages in conduct with intent to "annoy," "harass," or "alarm" the victim.\textsuperscript{110} Such a standard is more akin to the reasonable person standard since it does not require a credible threat. Arguably, when a stalker entices a third party to do the stalking, he has annoyed and harassed his victim. However, even if this argument is successfully made — which is yet to be seen — most of the state statutes that have this broad harassment standard only establish misdemeanors, not felonies.\textsuperscript{111}

\begin{itemize}
\item \textsuperscript{105} See, e.g., ARK. CODE ANN. § 5-71-229 (2006); FLA. STAT. § 836.10 (2006).
\item \textsuperscript{106} See, e.g., ARIZ. REV. STAT. ANN. § 13-2923 (2001) (requiring an actual threat when the perpetrator is not physically pursuing the victim); ARK. CODE ANN. § 5-71-229 (1997) (same); DEL. CODE ANN. tit. 11, § 1312A (2001 & Supp. 2003) (same).
\item \textsuperscript{108} See infra Part III.b.ii.
\item \textsuperscript{109} See infra Appendix.
\item \textsuperscript{110} See, e.g., HAW. REV. STAT. § 711-1106 (2003); IND. CODE § 35-45-10-1, -5(b)(1)(B) (2004); IOWA CODE § 708.7 (2003); ME. REV. STAT. ANN. tit. 17-A, § 210-A (2006).
\item \textsuperscript{111} See, e.g., ARK. CODE ANN. § 5-41-108(a), (b) (2006); CAL. PENAL CODE § 653m (West 1999); CONN. GEN. STAT. § 53a-183 (West 2005); DEL. CODE ANN. tit. 11, §§ 1311-1312 (2005); FLA. STAT. ANN. § 784.048 (2001); IOWA CODE § 708.7 (2003); KY. REV. STAT. ANN. § 525.080 (West 1999); MICH. COMP. LAWS § 750.411h (2004); MO. REV. STAT. § 565.225 (2000 & Supp. 2003); NEV. REV. STAT. ANN. § 200.575 (2003); S.C. CODE ANN. § 16-3-1700 (2003 & Supp. 2006).
\end{itemize}
The last category of state laws deal specifically with cyberstalking. As of January 2007, it appears that there are only six states (Illinois, Louisiana, Mississippi, North Carolina, Rhode Island, and Washington) that have enacted new "cyberstalking" statutes. Importantly, these states passed criminal laws specifically dealing with cyberstalking even though they already had offline stalking statutes with a "reasonable person standard" or a more general harassment standard. The enactment of these cyberstalking statutes illustrates an essential point; namely, these states recognized that offline stalking statutes, even if amended, are inadequate to deal with cyberstalking.

For example, Washington's offline stalking statute criminalizes conduct that the stalker "[k]nows or reasonably should know [would cause the person to be] afraid, intimidated, or harassed even if the stalker did not intend to place the person in fear or intimidate or harass the person." This Washington statute also applies to electronic communications. Even though Washington had a stalking statute with the reasonable person standard that applied to electronic communications, in 2004, lawmakers determined that the best way to deal with cyberstalking was to enact a law specifically addressing it. Other states should follow Washington's example.

115. WASH. REV. CODE § 9A.46.110(4).
117. Although New Mexico does not currently have any cyberstalking specific laws, it may not be far behind Washington. In 2004, the governor of New Mexico specifically addressed the issue by stating in his State of the State Address: "I also want to amend our stalking and harassment laws to prohibit electronic, or 'cyber' stalking." See Transcript of Gov. Bill Richardson's State Of The State Address, available at http://www.koat.com/politics/2779895/detail.html.
There are four other states (Florida, Nevada, Delaware, and Virginia) that have not enacted specific "cyberstalking" laws, but have amended their statutes in such a way so as to include many aspects of cyberstalking. The Florida Legislature, for example, recognized the dangers of relaxed cyberstalking laws, and amended the Florida stalking statute to provide criminal penalties for "[a]ny person who willfully, maliciously, and repeatedly follows, harasses, or cyberstalks another person." By definition, to "cyberstalk" means "to engage in a course of conduct to communicate, or to cause to be communicated, words, images, or language by or through the use of electronic mail or electronic communication, directed at a specific person, causing substantial emotional distress to that person and serving no legitimate purpose." A Florida district court expressly noted that the revised stalking/cyberstalking statute was "designed to protect women from being harassed . . . by ensuring that victims did not have to be injured or threatened with death before stopping a stalker's harassment." To fully address the gaps in state laws, state stalking statutes should be reviewed accordingly.

Although this third group of state laws which overtly deal with cyberstalking is clearly a step in the right direction, these statutes have gaps as well. Few of them explicitly address situations where the cyberstalker dupes an "innocent" third party to harass. The Illinois cyberstalking statute, for example, does not explicitly address incitement of third party harassment.


120. FLA. STAT. § 784.048(1)(d).


122. There is also a huge variety among the penalties for cyberstalking. For example, some statutes that could be construed to include cyberstalking are "harassment" statutes instead of "stalking" statutes. Generally, penalties for harassment are less than those for stalking. See Lee, supra note 84, at 379-80; Tucker, supra note 17, at 653. It is beyond the scope of this paper to consider what the penalties should be to address and deter cyberstalking crimes.

123. See FLA. STAT. § 784.048; 720 ILL. COMP. STAT. 5/12-7.5 (2002); NEV. REV. STAT. § 200.575(3) (2003); VA. CODE ANN. § 18.2-152.7:1 (2004); see also infra Appendix. But cf. COLO. REV. STAT. § 18-13-105 (2004) (not a stalking statute, but may apply to third party harassment).

124. 720 ILL. COMP. STAT. 5/12-7.5(b). The Illinois statute does criminalize a course of conduct which "alarms, torments, or terrorizes that person." Id. Although it has not yet been litigated, it could be argued that enticing a third party to "innocently" harass (e.g., posting false advertisements on alternative sexual websites) constitutes conduct which "alarms" and "terrorize" the victim.
Even more problematic are Louisiana’s and North Carolina’s cyberstalking statutes, which are almost identical to each other. Both of these statutes require that the harassing electronic communication be sent “to another.”125 Likewise, Mississippi’s cyberstalking statute also seems to suggest that the stalker has to specifically e-mail the victim.126 The Florida statute has similar problems since it requires that electronic communications be “directed at a specific person.”127 Although it has not yet been litigated, this may mean that the communication must be sent directly to the victim. Such requirements carve out cases where cyberstalkers dupe “innocent” third parties to do the harassment for them. It also may not reach cases like the Boyer case where terrifying messages were posted on a website, but were never sent directly to her.128

As of March 2007, only three states, Ohio,129 Rhode Island,130 and Washington,131 have statutes that explicitly address cases where third parties innocently harass the victim at the cyberstalker’s bidding. Thus, these three state statutes are the only current laws that likely deal with all aspects of cyberstalking.132

In sum, there are at least two ways to enact statutes that would fill the gaps in the state laws. The specific language of the statute that deals with the cyberstalker’s conduct should set forth an objective standard which focuses

128. HITCHCOCK, supra note 1, at 112.
129. OHIO REV. CODE ANN. § 2903.211(A)(2) (LexisNexis 2006) (“No person, through the use of any electronic method of remotely transferring information, including, but not limited to, any computer, computer network, computer program, or computer system, shall post a message with purpose to urge or incite another to commit a violation of division (A)(1) of this section.”) (emphasis added). This form of cyberstalking is only a misdemeanor, unless there was an actual threat. Id. § 2903.211(B)(1), B(2)(B).
130. R.I. GEN. LAWS § 11-52-4.2(a) (2002) (“Whoever transmits any communication by computer to any person or causes any person to be contacted for the sole purpose of harassing that person or his or her family is guilty of a misdemeanor . . . .”) (emphasis added).
131. WASH. REV. CODE § 9.61.260(1)(a) (Supp. 2004) (“A person is guilty of cyberstalking if he or she, with intent to harass, intimidate, torment, or embarrass any other person, and under circumstances not constituting telephone harassment, makes an electronic communication to such other person or a third party: Using any lewd, lascivious, indecent, or obscene words, images, or language, or suggesting the commission of any lewd or lascivious act.”) (emphasis added).
132. However, even these three laws do not specifically deal with e-mail bombs. Indeed, there are only three different statutes that overtly address e-mail bombs. 720 ILL. COMP. STAT. 135/1-2(a)(3.1) (2003); VT. STAT. ANN. tit. 13, § 1027(a)(ii) (1998); WASH. REV. CODE § 9.61.260(1)(b) (Supp. 2004).
on the victim's fear, rather than a subjective standard which focuses on the perpetrator's actions. Thus, cyberstalking statutes should adopt a reasonable person standard.\textsuperscript{133} Another way to address the gaps in the state statutes is to enact laws that specifically criminalize conduct where perpetrators use "innocent" third parties to do the harassment for them.

The inadequacies of current state cyberstalking stalking laws can be remedied foremost by being proactive, rather than a reactive. It took the Rebecca Schaeffer murder to rouse the enactment of stalking statutes. Hopefully, there does not have to be an equivalent cyberstalking case.\textsuperscript{134} State statutes should be enacted and revised now to deal with cyberstalking.

While many states are taking active steps to combat the problem of cyberstalking, there is a complete lack of uniformity in defining the crime. Conduct in one state that is criminal, may not be so in another.\textsuperscript{135} Moreover, there are instances where state laws may not be able reach the conduct at all; namely, where a stalker uses the Internet to stalk a victim in another state. In such instances, federal laws are paramount; however, they too have gaps.\textsuperscript{136}

\section*{B. Addressing the Gaps in Federal Laws}

There are three current federal laws which are applicable to cyberstalking. However, each of these laws, as currently interpreted, may fall short of adequately enabling the prosecution of cyberstalkers. This next section takes each of the three federal statutes, explains the law as applied to cyberstalking and considers whether they are inadequate to deal with the crime.

1. Gaps in the Interstate Communications Act, 18 U.S.C. § 875(c)

The Interstate Communications Act makes it a crime punishable by five years in prison to transmit "any communication" in interstate commerce con-
taining “any threat” to injure another person.\textsuperscript{137} “Any communication” includes threats transmitted across state lines via the telephone, e-mail, beepers, or the Internet.\textsuperscript{138} This statute successfully prosecuted at least one cyber-stalker who used the Internet to send threatening e-mail messages.\textsuperscript{139}

However, the requirement that the communication contain a “threat” is where this statute falls short because it is akin to a “credible threat” requirement. Thus, the statute would not be applicable to a cyberstalker who, absent a specific threat, uses the Internet to engage in a pattern of conduct intended to harass or annoy another.

\textit{United States v. Alkhazae}\textsuperscript{140} is a prime example of why the “threat” requirement is problematic. In this case, the defendant e-mailed numerous messages to an acquaintance that included violent sexual fantasies about women and young girls.\textsuperscript{141} The defendant eventually posted an explicitly “depraved torture-and-snuff story” on a chat room where the rape-victim had the same name as one of his classmates.\textsuperscript{142} Despite the sadistic story about the defendant’s classmate, the court held that he was not in violation of § 875(c), because he did not make a “communication[s] containing a threat.”\textsuperscript{143}

Because this statute is limited to only those cyberstalking cases where there has been a “true” (e.g., credible) threat, it does not address the many situations where the cyberstalker engages in conduct intended to harass the victim, but without making explicit threats.


The Telephone Harassment Statute\textsuperscript{144} was passed in 1934; a time when the telephone, much like the Internet now, was the cutting edge technology of communication. The statute makes it a crime, punishable by up to two years in prison, to anonymously and knowingly make a telephone call, or use a “telecommunications device,” “to annoy, abuse, threaten, or harass” a person.\textsuperscript{145}

In January 2006, the federal government attempted to respond to the cyberstalking problem by trying to ensure that e-mail messages sent via the Internet were covered by § 223. In the voluminous “Violence Against

\textsuperscript{137} 18 U.S.C. § 875(c) (2006).
\textsuperscript{138} \textit{Id}\textsuperscript{.}
\textsuperscript{139} See United States v. Kammersell, 196 F.3d 1137 (10th Cir. 1999) (upholding the defendant’s conviction even though the defendant sent the e-mail messages to the victim who was in the same state because the e-mail message was sent via interstate telephone lines).
\textsuperscript{140} 104 F.3d 1492 (6th Cir. 1997).
\textsuperscript{141} \textit{Id} at 1493.
\textsuperscript{142} \textit{Id} at 1498 (Krupansky, J., dissenting).
\textsuperscript{143} \textit{Id} at 1496 (alteration in original).
\textsuperscript{145} \textit{Id} § 223(a)(1)(C).
Women Act" a section entitled, "Preventing Cyberstalking," amended the statute to apply to e-mail messages. Specifically, the definition of the "telecommunications device" was changed to include "any device or software that can be used to originate telecommunications or other types of communications that are transmitted, in whole or in part, by the Internet."

While the amendment changed the definition of a "telecommunications device" to specifically include e-mail, it did not change any of the required elements. Thus, for the statute to be triggered, the cyberstalker would still have to anonymously and knowingly send a message via the Internet "to annoy, abuse, threaten, or harass" a person. The amendment created some controversy. Proponents called it an answer to many victims’ cries for help. But, some critics have complained that the term “annoy” is too overbroad because it “might characterize a wide range of anonymous Internet banter that falls far short of cyberstalking.”

However, it seems unlikely that the amendment would create any constitutional problems that the courts have not already dealt with. For example, in United States v. Bowker, the Sixth Circuit found that the word “annoy” in the statute was not unconstitutional because: (1) it upheld Congressional in-


148. Violence Against Women Act, supra note 146.

149. Id. (adding this language to 47 U.S.C. § 223(h)(1)(C)).

150. Even without this amendment, the courts may have interpreted the Internet as a “telecommunication device.” See ACLU v. Reno, 929 F. Supp. 824, 828-29 (E.D. Pa. 1996) (“Clearly, the sponsors of the CDA [47 U.S.C. § 223(a)(1)(B)] thought it would reach individual Internet users, many of whom still connect through modems.”).


153. 372 F.3d 365 (6th Cir. 2004), vacated on other grounds, 543 U.S. 1182 (2005) (upholding criminal convictions, but remanding to district court for resentencing). See also United States v. Lampley, 573 F.2d 783 (3d Cir. 1978) (upholding constitutionality of the statute).
tent to "protect innocent individuals from fear" without being vague or over-

broad; and (2) it did not chill political or free speech.\footnote{Bowker, 372 F.3d at 382-83. The court explained that the word "annoy" standing alone might pose vagueness concerns. Id. at 382. But, the statutory language must be read in the context of Congressional intent to protect innocent individuals from fear, abuse or annoyance at the hands of persons who employ the telephone, not to communicate, but for other unjustifiable motives. This context suggests that the words annoy, abuse, threaten or harass should be read together to be given similar meanings. Id. at 382-83 (citation omitted). Thus, "[a]ny vagueness associated with the word 'annoy' is mitigated by the fact that the meanings of 'threaten' and 'harass' can easily be ascertained and have generally accepted meanings." Id. at 383. The court went on to explain that the statute did not violate the freedom of speech because the "thrust of the statute is to prohibit communications intended to instill fear in the victim, not to provoke a discussion about political issues of the day." Id. at 379.} Although Bowker was decided prior to the amendment to § 223, the analysis is the same. Read in context, "annoy," like "threaten" and "harass," is not unconstitutional because its purpose is to prohibit messages aimed at instilling fear, whether the message is sent via the telephone or the Internet.

This amendment to § 223 is a step in the right direction since it is evidence that Congress has specifically recognized cyberstalking as a problem. However, even with the amendment, § 223 is still inadequate to fully deal with cyberstalking for three reasons. First, the identity of the person sending the message must be anonymous.\footnote{47 U.S.C. § 223(a)(1)(C) (2006). See also Jones, supra note 153 (citing Jeff Lundgren, communications director for the U.S. House Judiciary Committee, who said that the amendment "doesn't target any Internet except e-mail").} It seems odd to only make cyberstalking a crime where the identity of the cyberstalker is unknown.\footnote{However, one court has held that the lack of the anonymity element made a state statute unconstitutional under the New Hampshire State Constitution. See State v. Brobst, 857 A.2d 1253, 1256-57 (N.H. 2004) However, this case did not deal with the constitutionality of the statute under the U.S. Constitution.} This element seemingly, and without reason, carves out a number of terrifying cases where the victim knows the identity of the cyberstalker.

Second, the statute applies only to direct communications between the stalker and victim, e.g., the statute would only be triggered when the cyberstalker sends an e-mail directly to the victim.\footnote{47 U.S.C. § 223(a).} Thus, the amended statute is inadequate to deal with behavior where the cyberstalker indirectly harasses or terrorizes his victim by posting messages on a bulletin board, creating a Web site aimed at terrorizing his victim, or encouraging third parties to harass the victim.

Finally, the statute limits cyberstalking to the maximum punishment of two years in prison.\footnote{Id. § 223(a).} While there may be cyberstalking cases where the actions merit a sentence of only two years, there are certainly federal statutes...
that make offline stalking punishable by five years to life imprisonment.159 It is not clear why there should be such low limits on the punishment of a crime under this statute.

Thus, the statute, even with the amendment, fails to fully combat all of the criminal vices of cyberstalking.


The most promising federal statute to combat cyberstalking is the “Interstate Stalking Punishment and Prevention Act.”160 The statute was passed in 1996 and was the first federal law to deal specifically with stalking (and, at that time, specifically offline stalking). Initially, there were three elements to the statute: (1) the defendant had to “travel across state lines” (2) and intentionally “engage in a course of conduct” using “mail or any facility of interstate or foreign commerce” (3) that placed a person in “reasonable fear of death” or of “serious bodily injury.”161 There have been two recent amendments to this statute that makes it applicable to some forms of cyberstalking.

The first amendment, passed in 2000, changed the first element of the statute dealing with jurisdiction. Before the amendment, the statute was only triggered when a stalker physically traveled “across state lines,” which obviously posed a problem in cyberstalking cases since a cyberstalker can harass his victim without even walking out of his front door, let alone travel across state lines. However, the 2000 amendment changed the applicability of the statute from a person who physically travels to a person who “travels in interstate or foreign commerce.”162 While it has not been specifically litigated whether traveling in interstate commerce for the purpose of the statute encompasses the Internet, there has been one Sixth Circuit case since the amendment where the defendant was charged with online stalking under § 2261A;163 however, in that case the defendant had traveled across state lines.164

160. 18 U.S.C. § 2261A.
161. Id. § 2261A (Supp. II 1996).
163. United States v. Bowker, 372 F.3d 365, 370 (6th Cir. 2004), vacated on other grounds, 543 U.S. 1182 (2005). In Bowker, the defendant was charged with “Count 2 (cyberstalking),” which alleged “that between December 25, 2000 and August 18, 2001 Bowker, located in Ohio, knowingly and repeatedly used the internet to engage in a course of conduct that intentionally placed Knight, then located in West Virginia, in reasonable fear of death or serious bodily injury, in violation of 18 U.S.C. § 2261A(2).” Id. at 377.
164. Id. at 374.
The second amendment to § 2261A occurred recently in January 2006. The "Violence Against Women Act" (the same act that amended the Telephone Harassment Statute) added language to both the second and third elements criminalizing a course of conduct where the stalker "uses . . . any interactive computer service" that causes "substantial emotional distress." The new language of the statute has not yet been litigated, but it is arguable that "interactive computer service" reaches cases in which cyberstalkers use the computer to send e-mail messages, anonymous or not, or post messages on blogs or Websites.

Thus, the newly amended § 2261A addresses many of the shortcomings of the other federal statutes. It does not have a "true/credible threat" requirement; but rather adopts a standard that measures the victim's "reasonable fear" or "substantial emotional distress." Nor does it limit coverage of the "use" of the computer to only anonymous e-mail messages.

However, § 2261A still falls short of completely addressing the cyberstalking problem. The statute does not squarely deal with situations where the cyberstalker pretends to be the victim and encourages third parties to innocently harass the victim, such as posting sexual invitations on a message board in the name of the victim to dupe third parties to respond.

The bottom line is that the current federal laws are not able to deal with all the criminal aspects of cyberstalking. But they should. Particularly because of the jurisdictional problems that cyberstalking creates. And, the evidence to prosecute the cyberstalkers, or even find them, may be with Internet providers in all different jurisdictions. Better federal laws will give the federal authorities the necessary tools to control and combat cyberstalking.

C. Potential Statutory Barriers

In addition to gaps in the state and federal laws, there may also be barriers in combating the cyberstalking problem. In particular, the problems that plague the codification of cyberstalking could also create significant difficulties for victims attempting to obtain protective orders against cyberstalkers. The main reason for this problem is that often the statutory definition of "stalking" governs the issuance of protective orders. Thus, where the language of the statute does not cover cyberstalking, it may be difficult to obtain a protective order. Also, the application procedure for a protective order may

165. Violence Against Women Act, supra note 146.
166. Id. § 114(a).
cyberstalking, a new crime

Call for information that is difficult or impossible to obtain due to the anonymous nature of a cyberstalker. In Virginia, for example, the law provides that a Stalking Protective Order may be issued after a criminal conviction for stalking. Alternatively, the victim would have to prove by a preponderance of the evidence that the perpetrator is guilty of stalking. This may pose a problem in cyberstalking cases, because it is unlikely that the Virginia stalking statute covers cases where the cyberstalkers entice third party harassment. In fact, it is unclear if Virginia’s stalking statute specifically covers electronic communications. Thus, cyberstalking victims may have to wait until the cyberstalker is formally prosecuted before they can secure any sort of protective order.

Federal stalking laws pose similar problems. In the last decade, federal congressional bills have been introduced, but not passed, that would require protective orders be issued upon conviction of stalking. The Victims of Trafficking and Violence Act, which partially strengthened existing federal laws concerning cyberstalking, failed to retain the requirement that protective orders be issued upon conviction. Indeed, that Act did not address issues re-

---

171. For example, to file a Petition for Order of Protection in Indiana, the victim must know (1) the correct name of the cyberstalker, (2) either their date or birth or their social security number, and (3) a correct, current address. See IND. CODE § 34-26-5 (2004); see also Instructions for Petition for Order of Protection – Filed by Person Seeking Protection, http://www.in.gov/judiciary/forms/po/po/po-0102.doc (last visited May 23, 2007). The anonymity of the Internet may make it difficult under such a statute to procure all this detailed information; thus, a cyberstalking victim may be unable to receive any official protection from the stalking.

172. See VA. CODE ANN. § 18.2-60.3(D) (2004).

173. Id. § 19.2-152.9(D).

174. Id. § 18.2-60.3.

175. Id. See infra Appendix.

176. There are other examples where it would be hard for cyberstalking victims to obtain protective orders. In Las Vegas, victims may apply for a protective order only if they are either (1) related by blood or marriage to the stalker, (2) have been in a dating relationship with or been a roommate of the stalker, or (3) have children with the stalker. See Las Vegas Metropolitan Police Department—Domestic Violence, http://www.lvmpd.com/bureaus/dv_protective.html (last visited May 23, 2007). Likewise in Texas, “[t]o obtain a protective order, the victim and the offender must be (1) related by blood or marriage, (2) living together, or previously lived together, or (3) have a child together.” Attorney General of Texas Greg Abbott, Jan. 30, 2007, http://www.oag.state.tx.us/victims/protective.shtml#law (last visited May 23, 2007). The protective order is defined in terms of family violence, and makes no mention of resources for cyberstalking. Id. In Maryland, victims must prove that an act occurred that caused them to fear imminent bodily harm (e.g., a credible threat) or prove criminal stalking to obtain a peace or protective order. Peace and Protective Orders, Oct. 2005, http://www.courts.state.md.us/courtforms/joint/ccdcdv01br.pdf (last visited May 23, 2007).

lated to protective orders in cyberstalking cases at all.\textsuperscript{178} Thus, a cyberstalking victim may not be able to obtain a protective order via current federal laws.

Another potential issue concerns \textit{how} a cyberstalker subscribes to the Internet. For instance, the Federal Cable Communications Policy Act prohibits the disclosure of cable subscriber records to law enforcement agencies without a court order and advance notice to the subscriber.\textsuperscript{179} Potentially this means that if the perpetrator uses a cable connection, as opposed to a dial-up connection or any service that uses the telephone lines, to access the Internet, law enforcement agents have to notify the potential cyberstalker before being able to access computer records (\textit{e.g.}, evidence that would be crucial to prosecuting a cyberstalker). Although it has not been litigated in a cyberstalking case, it seems as though the Patriot Act would likely give the court some leeway in allowing the government to access cable records without first notifying the cyberstalker.\textsuperscript{180} While this might help gather evidence in cyberstalking cases, since the Patriot Act was not specifically enacted to deal with cyberstalking, it seems that a better option would be to deal head-on with issues raised by statutes that relate to stalking and the internet. Simply put, laws need to be enacted, or at least updated, in order to adequately deal with cybercrimes in this new internet age.

\begin{footnotesize}
\begin{itemize}
\item \textsuperscript{179} Cable Communications Policy Act of 1984, 47 U.S.C. § 551(h) (2006).
\item \textsuperscript{180} See, \textit{e.g.}, Patriot Act of 2001, Pub. L. No. 107-56 (2001); \textit{See In re Application of the United States for an Order Pursuant to 18 U.S.C. § 2703(D) Directed to Cablevision Sys. Corp. 1111 Steward Ave., Bethpage, N.Y. 11714, 158 F. Supp. 2d 644, 648-49 (D. Md. 2001). In In re Application, the court ruled that the part of CCPA that required cable operators to give advance notice to their subscribers before revealing their information to the government was repealed by implication by the more recent Electronic Communications Privacy Act. \textit{Id.;} 18 U.S.C. § 2705(b) (2006). Although In re Application was not a cyberstalking case, it seems as though the same argument could be applied. Moreover, since this case, the Patriot Act has come on the scene. Although it has not yet been litigated, the Patriot Act appears to be an even broader abolition of the CCPA requirement. The Patriot Act specifically amended the language in subsection (c)(2)(D) of the CCPA, which effectively allows the government to obtain information without a court order. \textit{See} Patriot Act of 2001, Pub. L. No. 107-56 § 211, 115 Stat. 272, 283-84; \textit{see also} 18 U.S.C. §§ 119, 121, 206 (2006) (These chapters include all sections of the code for Wire and Electronic Communications Interception and Interception of Oral Communications; Stored Wire and Electronic Communications and Transactional Records Access; and Pen Registers and Trap and Trace Devices). Therefore, the Patriot Act has given the government more leeway in obtaining subscriber information from cable providers by getting rid of the court order, and In re Application might allow for this information to be gathered without notification to the subscriber even if a court order is sought.
\end{itemize}
\end{footnotesize}
V. PROBLEMS WITH CRIMINALIZING CYBERSTALKING

There are at least two potential concerns related to criminalizing cyberstalking. First, anytime speech is involved, many constitutional issues arise. Second, to date, the cyberstalking data that has been collected is somewhat uncertain. While each of these potential concerns merit more discussion, they do not create a complete barrier to criminalizing cyberstalking.

A. Constitutional Considerations

As with offline harassment laws, cyberstalking laws need to be relatively broad to be effective. However, they cannot be so broad as to impinge upon the rights of free speech protected under the First Amendment. Thus, any interpretation of existing harassment laws and changes in stalking statutes should keep in mind that, as with offline stalking, cyberstalking should generally involve conduct reasonably understood to constitute harassing and threatening behavior.\(^{181}\)

Court rulings regarding the constitutionality of telephone harassment laws give guidance. Constitutional concerns are not implicated when statutes prohibit the matter and means of the telephone call and have an element of specific intent to harass the person called. Thus, telephone harassment statutes that have a specific intent element are constitutional when they prohibit repeated, anonymous, or late-night calls.\(^{182}\) Likewise, statutes related to cyberstalking should focus on specific intent, conduct-based behavior such as repeated transmission of e-mails (e-mail “letter bombs”), or use of lewd language with the intent to harass.\(^{183}\)

Thus, as long as statutes aimed at cyberstalking contain the following two elements, it will probably not be unconstitutionally vague or overbroad: (1) “willfully” harasses, follows, engages in conduct, etc. ensures that the perpetrator has the requisite specific intent to commit a crime, and (2) a provision stating that the law does not include “constitutionally protected activity,” including, but not limited to “picketing and organized protests.”\(^{184}\) Moreover, many current offline stalking statutes contain specific language that the statute cannot violate constitutional rights.\(^{185}\) This may be another element that should be included in newly enacted cyberstalking statutes.


\(^{183}\) Id. at 526.

\(^{184}\) Tucker, supra note 17, at 622, 630-31.

\(^{185}\) GA. CODE ANN. § 16-5-92 (2003); IDAHO CODE ANN. § 18-7906(2)(a) (2004); IND. CODE § 35-45-10-1 (2004); KY. REV. STAT. § 508.130(2) (West 1999);
B. Lack of Cyberstalking Data

Second, evidence of whether cyberstalking is indeed becoming a societal problem is largely anecdotal and informal. In fact, law enforcement agencies from different jurisdictions report widely different statistics on stalking via the Internet. However, those jurisdictions that have computer crime departments tend to report a larger number of cyberstalking incidents.\textsuperscript{186} The lack of data is partly because many cyberstalking victims do not report the conduct to law enforcement, and partly because law enforcement agencies have not had adequate training in how to deal with it.\textsuperscript{187} However, there are some reports that suggest that cyberstalking is ever-growing. The CyberAngels, a non-profit organization that assists cyberstalking victims,\textsuperscript{188} estimates that there are approximately 63,000 Internet stalkers in the United States and 474,000 victims world-wide.\textsuperscript{189}

VI. CONCLUSION

As technology changes, so should the laws. For example, with the increased and daily use of cars, the laws had to change to make driving under the influence of alcohol a crime. Similarly, the stalking and harassment laws should be reviewed to ensure that they are adequate to address the new crime of cyberstalking.

Cyberstalking is a crime with issues that are distinct from offline stalking such that current state and federal laws are inadequate to deal with all aspects of cyberstalking. Thus, cyberstalking laws should be enacted that have the reasonable person standard and also explicitly deal with situations where the cyberstalker dupes “innocent” third parties to do the stalking.

Clear federal and state laws which specifically prohibit cyberstalking may address this problem. If victims knew of the laws, they might be more encouraged to report incidents. And, if cyberstalkers knew of the laws, they might be less likely to stalk victims online. Moreover, clear cyberstalking laws would give guidance to law enforcement agencies on how to appropriately respond to reported incidents.


\textsuperscript{187} 1999 REPORT ON CYBERSTALKING, supra note 29, at 9, 12.

\textsuperscript{188} Id. at 9.

\textsuperscript{189} The CyberAngels Website is at www.cyberangels.org.

\textsuperscript{189} 1999 REPORT ON CYBERSTALKING, supra note 135, at 7 n.4.
At the end of the day, it is important to recognize that the new age of the internet is creating a host of cybercrimes; cyberstalking is one of them. Statues should be evaluated to ensure the technology, as fast-paced as it is, does not go beyond the reach of the law.

**APPENDIX (STARTS ON NEXT PAGE)**
## APPENDIX: STATE STATUTES

<table>
<thead>
<tr>
<th>Code</th>
<th>Alabama</th>
<th>Alabama</th>
<th>Alaska</th>
<th>Alaska</th>
<th>Arizona</th>
</tr>
</thead>
<tbody>
<tr>
<td>Title</td>
<td>Harassing Communications (misdemeanor)</td>
<td>Stalking (felony)</td>
<td>1st Degree Stalking</td>
<td>2nd Degree Stalking</td>
<td>Harassment</td>
</tr>
<tr>
<td>Reasonable Person Standard?</td>
<td>Yes, but requires a “threat”</td>
<td>Yes, but requires a “credible threat.”</td>
<td>No</td>
<td>No</td>
<td>“Conduct directed at a specific person which would cause a reasonable person to be seriously alarmed, annoyed or harassed and the conduct in fact seriously alarms, annoys or harasses the person.”</td>
</tr>
</tbody>
</table>

### Credible Threat Standard?

- Requires a “threat”
- Yes
- No
- Yes, requires a “threat” of physical injury or sexual contact
<table>
<thead>
<tr>
<th>Requires Actual Physical Pursuit?</th>
<th>No</th>
<th>No</th>
<th>No</th>
<th>No</th>
<th>No</th>
</tr>
</thead>
<tbody>
<tr>
<td>Statute Covers Electronic Communications?</td>
<td>Yes</td>
<td>No</td>
<td>Yes, but only covers “electronic communications” to victim. See ALASKA STAT. §§ 11.41.260 to 41.270(3)(f) (2006).</td>
<td>Yes, but only to “electronic communications” to victim</td>
<td></td>
</tr>
</tbody>
</table>

### Notes

**Potential Statutory Problems in prosecuting cyberstalking**

1. Requires a threat.
2. May not apply when a cyberstalker dupes an “innocent” third party to harass.

1. Requires a threat.
2. May not apply when a cyberstalker dupes an “innocent” third party to harass.

1. May only apply to e-mail sent directly to the victim, not other Internet postings.
2. May not apply when a cyberstalker dupes an “innocent” third party to harass.

1. May only apply to e-mail sent directly to the victim, not other Internet postings.
2. May not apply when a cyberstalker dupes an “innocent” third party to harass.

1. May not apply when a cyberstalker dupes an “innocent” third party to harass.
<table>
<thead>
<tr>
<th>Code</th>
<th>Arizona</th>
<th>Arkansas</th>
<th>Arkansas</th>
<th>Arkansas</th>
<th>California</th>
</tr>
</thead>
<tbody>
<tr>
<td>Title</td>
<td>Stalking</td>
<td>Stalking (felony)</td>
<td>No</td>
<td>No</td>
<td>Yes, but also requires a credible threat</td>
</tr>
<tr>
<td>Reasonable Person Standard?</td>
<td>Yes, but only when the conduct includes repeatedly maintaining a visual or physical proximity to a person, otherwise a threat is required.</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes, but also requires a credible threat</td>
</tr>
<tr>
<td>Credible Threat Standard?</td>
<td>Sometimes Conduct includes repeatedly maintaining a visual or physical proximity to a person conveying verbal or written threats or threats implied by conduct.</td>
<td>Yes “Terrorist threat”</td>
<td>No, requires intent to annoy</td>
<td>Sometimes “Message threatens to cause injury to any person or damage to any property of any person or uses obscene, lewd, or profane language”</td>
<td>Yes “Verbal or written threat including electronic statements and conduct, combined with a pattern of conduct intending to cause fear, and made with the apparent ability to carry out the threat as to cause the target”</td>
</tr>
<tr>
<td>Requires Actual Physical Pursuit?</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>----------------------------------</td>
<td>----</td>
<td>----</td>
<td>----</td>
<td>----</td>
<td>----</td>
</tr>
<tr>
<td>Notes</td>
<td>Requires an actual threat when the perpetrator is not physically pursuing the victim. 1. Requires an actual threat when the perpetrator is not physically pursuing the victim. 2. May not apply when a cyberstalker dupes an “innocent” third party to harass.</td>
<td>1. Requires a threat. 2. May not cover electronic communications. 3. May not apply when a cyberstalker dupes an “innocent” third party to harass.</td>
<td>1. May only apply to messages sent directly to the victim (e-mail), not other Internet postings 2. May not apply when a cyberstalker dupes an “innocent” third party to harass.</td>
<td>1. May only apply to messages sent directly to the victim (e-mail), not other Internet postings 2. May not apply when a cyberstalker dupes an “innocent” third party to harass.</td>
<td>1. Requires a credible threat. 2. May not apply when a cyberstalker dupes an “innocent” third party to harass.</td>
</tr>
</tbody>
</table>

Goodno: Goodno: Cyberstalking, a New Crime

Published by University of Missouri School of Law Scholarship Repository, 2007

to reasonably fear for her safety or her family’s safety"
<table>
<thead>
<tr>
<th>Code</th>
<th>California</th>
<th>Colorado</th>
<th>Colorado</th>
<th>Connecticut</th>
<th>Connecticut</th>
</tr>
</thead>
<tbody>
<tr>
<td>Title</td>
<td>Telephone Calls or Contact by Electronic Communication Device with Intent to Annoy (misdemeanor)</td>
<td>Harassment Stalking</td>
<td>Criminal Libel (felony)</td>
<td>1st Deg. Stalking (felony)</td>
<td>2nd Deg. Stalking (misdemeanor)</td>
</tr>
<tr>
<td>Reasonable Person Standard?</td>
<td>No</td>
<td>Yes (Stalking)</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Credible Threat Standard?</td>
<td>No</td>
<td>Yes (Stalking)</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Requires Actual Physical Pursuit?</td>
<td>No</td>
<td>Yes (Stalking)</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Statute Covers Electronic Communications?</td>
<td>Yes, but only applies to &quot;contact&quot; with the victim</td>
<td>Possibly (Stalking)</td>
<td>The statute specifically notes seriousness of stalking.</td>
<td>Not specifically, but applies to &quot;written instrument&quot;</td>
<td>&quot;follows or lies in wait&quot;</td>
</tr>
<tr>
<td>Notes</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Potential Statutory Problems

1. Reasonable standard would be more applicable.
2. May not apply when a cyberstalker dupes an "innocent" third party to harass.

See § 18-9-111(4)(a).

1. May not apply when a cyberstalker dupes an "innocent" third party to harass.
2. Electronic communications are not specifically covered.
3. May not apply when a cyberstalker dupes an "innocent" third party to harass.

1. This is not a stalking statute, but might be interpreted to cover "innocent" third party harassment, if "public hatred" includes the Internet.
2. Electronic communications are not specifically covered.
3. May not apply when a cyberstalker dupes an "innocent" third party to harass.

1. Electronic communications are not specifically covered.
2. Requires physical pursuit, which would not include many aspects of cyberstalking.
3. May not apply when a cyberstalker dupes an "innocent" third party to harass.
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Title</td>
<td>3rd Deg. Stalking (misdemeanor)</td>
<td>1st Deg. Harassment (felony)</td>
<td>2nd Deg. Harassment (misdemeanor)</td>
<td>Stalking (felony or misdemeanor)</td>
</tr>
<tr>
<td>Reasonable Person Standard?</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Credible Threat Standard?</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Requires Actual Physical Pursuit?</td>
<td>Yes “follows or lies in wait”</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Statute Covers Electronic Communications?</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>Covers “computer network”</td>
<td></td>
<td></td>
<td>Communicate with a person by electronic communication in a manner which the person knows is likely to cause</td>
</tr>
</tbody>
</table>
Notes

Potential Statutory Problems

1. Electronic communications are not explicitly covered.
2. Requires physical pursuit, which would not include many aspects of cyberstalking.
3. May not apply when a cyberstalker dupes an “innocent” third party to harass.

Broad statute covering communications made “in a manner likely to cause annoyance or alarm.”

1. Requires direct contact with the victim.
2. May not apply when a cyberstalker dupes an “innocent” third party to harass.
3. May only apply to messages sent directly to the victim (e-mail), not other Internet postings.

1. May not apply when a cyberstalker dupes an “innocent” third party to harass.
2. Requires a threat when the perpetrator is not physically pursuing the victim.
3. May only apply to messages sent directly to the victim (e-mail), not other Internet postings.

annoyance or alarm
For a misdemeanor charge, the statute is broad covering any “course of alarming or distressing conduct which serves no legitimate purpose;” the language is narrower for a felony charge. Compare § 1311 with § 1312.
1. For a felony charge, it may not apply when a cyberstalker dupes an “innocent” third party to harass.
2. For a felony charge, it may only apply to messages sent directly to the victim (e-mail), not other Internet postings.
<table>
<thead>
<tr>
<th>Code</th>
<th>District of Columbia</th>
<th>Florida</th>
<th>Florida</th>
<th>Georgia</th>
<th>Georgia</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reasonable Person Standard?</td>
<td>Yes</td>
<td>But, for a felony charge requires a credible threat.</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Credible Threat Standard?</td>
<td>No</td>
<td>No - misdemeanor stalking</td>
<td>Yes</td>
<td>Conduct that “harass[es] or intimi-dat[es].” § 16-5-90(a). No</td>
<td>No</td>
</tr>
<tr>
<td>Requires Actual Physical Pursuit?</td>
<td>No</td>
<td>No - felony stalking</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Statute Covers Electronic Communications?</td>
<td>Unclear, does not specify how the communication must be made</td>
<td>Yes</td>
<td>Not specifically, but does cover “inscribed communication”</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>
Section 784.048(1)(d) specifically includes cyberstalking (amended 2003). “Cyberstalk” means to engage in a course of conduct to communicate, or to cause to be communicated, words, images, or language by or through the use of electronic mail or electronic communication, directed at a specific person, causing substantial emotional distress to that person and serving no legitimate purpose.”

Florida has a model statute that seems to cover most aspects of cyberstalking; unclear if “directed at a specific person” limits the statute’s reach to communications sent directly to the victim.

1. Unclear if electronic communications are covered.
2. May not apply when a cyberstalker dupes an “innocent” third party to harass.

1. Unclear if electronic communications are covered.
2. Requires a credible threat.
3. May not apply when a cyberstalker dupes an “innocent” third party to harass.

1. May not apply when a cyberstalker dupes an “innocent” third party to harass.
2. May only apply to direct contact with the victim (e-mail), not other Internet postings.

1. May not apply when a cyberstalker dupes an “innocent” third party to harass.
2. May only apply to direct contact with the victim (e-mail), not other Internet postings.

Computer and computer network defined by GA. CODE ANN. § 16-9-92 (2003); contact occurs at the place or places where the communication is received.
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Hawaii HAW. REV. STAT. §§ 711-1106.4 to -1106.5 (2003).</td>
<td>Harassment by Stalking</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Hawaii HAW. REV. STAT. §§ 711-1106 (2003).</td>
<td>Harassment</td>
<td>Yes</td>
<td>Not specifically, but see “Notes”</td>
<td>No</td>
<td>Yes (either reasonable person or credible threat)</td>
</tr>
<tr>
<td>Idaho IDAHO CODE ANN. §§ 18-7905 to -7906 (2004).</td>
<td>1st Deg. Stalking</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>Yes (either reasonable person or credible threat)</td>
</tr>
<tr>
<td>Illinois 720 ILL. COMP. STAT. 5/12-7.5 (2002).</td>
<td>Cyberstalking (felony)</td>
<td>Yes</td>
<td>Yes (either reasonable person or credible threat)</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Illinois 720 ILL. COMP. STAT. 135/1-2 (2003).</td>
<td>Harassment Through Electronic Communications</td>
<td>Yes</td>
<td>Yes (either intent to harass or direct threat)</td>
<td>Yes</td>
<td>Yes Same as 720 ILL. COMP. STAT. 5/12-7.5 (2002).</td>
</tr>
</tbody>
</table>
Aggravated harassment by stalking requires a current and prior conviction for the offense of harassment by stalking.


May apply when a cyberstalker dupes an “innocent” third party to harass.

May apply when a cyberstalker dupes an “innocent” third party to harass

May apply when a cyberstalker dupes an “innocent” third party to harass

Statute prohibits knowingly inducing a person to transmit a harassing message to a person under 13. See § 135/1-2(3.1). Note this requires direct communication with the victim.

1. May not apply when a cyberstalker dupes an “innocent” third party to harass.

1. May require threat.

1. May not apply when a cyberstalker dupes an “innocent” third party to harass.

1. May only apply to direct contact with the victim (e-mail), not other Internet postings.

1. May not apply when a cyberstalker dupes an “innocent” third party to harass.

Illinois has a model statute that seems to cover most aspects of cyberstalking.

Illinois has a model statute that seems to cover most aspects of cyberstalking, including e-mail bombs. See § 135/1-2(3).
<table>
<thead>
<tr>
<th>Code</th>
<th>Indiana</th>
<th>Indiana</th>
<th>Iowa</th>
<th>Iowa</th>
<th>Kansas</th>
</tr>
</thead>
<tbody>
<tr>
<td>Title</td>
<td>Stalking (felony)</td>
<td>Harassment (misdemeanor)</td>
<td>Harassment</td>
<td>Stalking</td>
<td>Stalking</td>
</tr>
<tr>
<td>Reasonable Person Standard?</td>
<td>Yes</td>
<td>No, but has broad standard that covers the intent “to harass”</td>
<td>No, but has broad standard that covers the intent “to harass”</td>
<td>Yes, for first and second degree harassment</td>
<td>Yes, requires a threat. See § 708.11(1)(b), 2(a).</td>
</tr>
<tr>
<td>Credible Threat Standard?</td>
<td>Yes, for a felony. See IND. CODE § 35-45-10-5(b)(1)(B).</td>
<td>No</td>
<td>Yes, for first and second degree harassment</td>
<td>No, for third degree harassment</td>
<td>Yes, either visual proximity or threat</td>
</tr>
<tr>
<td>Requires Actual Physical Pursuit?</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes, either visual proximity or threat</td>
<td>No</td>
</tr>
<tr>
<td>Statute Covers Electronic Communications?</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Not specifically</td>
<td>Yes</td>
</tr>
<tr>
<td>Notes</td>
<td>Sometimes requires personal contact—an encounter where two or more people are in visual or</td>
<td></td>
<td></td>
<td>Electronic communication includes, but is not limited to, computers and computer networks</td>
<td></td>
</tr>
</tbody>
</table>
Potential Statutory Problems

1. May not apply when a cyberstalker dupes an “innocent” third party to harass.
2. Requires a threat for conduct to be a felony.

1. May not apply when a cyberstalker dupes an “innocent” third party to harass.
2. May only apply to direct contact with the victim (e-mail), not other Internet postings. § 35-45-2-2(a)(4)(A)-(B).

1. Requires a threat.
2. May not apply when a cyberstalker dupes an “innocent” third party to harass.
3. May not apply when a cyberstalker dupes an “innocent” third party to harass.
<table>
<thead>
<tr>
<th>Code</th>
<th>Kentucky</th>
<th>Kentucky</th>
<th>Louisiana</th>
<th>Louisiana</th>
<th>Maine</th>
<th>Maryland</th>
</tr>
</thead>
<tbody>
<tr>
<td>Title</td>
<td>1st Deg. Stalking</td>
<td>Harassing Communications (misdemeanor)</td>
<td>Stalking</td>
<td>Cyberstalking</td>
<td>Terrorizing (§ 210) Stalking (§ 210A)</td>
<td>Misuse of Electronic Mail</td>
</tr>
<tr>
<td>Reasonable Person Standard?</td>
<td>Yes, but also requires an explicit threat</td>
<td>No, but has broad standard that covers the intent “to harass”</td>
<td>No, but has broad standard that covers the intent “to harass”</td>
<td>Yes, but requires threat.</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>Credible Threat Standard?</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes Conduct requires either visual proximity or a threat</td>
<td>No</td>
</tr>
<tr>
<td>Requires Actual Physical Pursuit?</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Statute Covers Electronic Communications?</td>
<td>No</td>
<td>Yes</td>
<td>Unclear</td>
<td>Yes</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>-----------------------------------------</td>
<td>----</td>
<td>-----</td>
<td>---------</td>
<td>-----</td>
<td>-----</td>
<td></td>
</tr>
<tr>
<td>E-mail means transmission by computer or other electronic means received by a person with a unique address</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Notes

**Potential Statutory Problems**

1. Requires a threat.
2. May not cover electronic communications.
3. May not apply when a cyberstalker dupes an "innocent" third party to harass.

1. May only apply to direct contact with the victim (e-mail), not other Internet postings.
2. May not apply when a cyberstalker dupes an "innocent" third party to harass.

1. May not cover electronic communications.
2. May not apply when a cyberstalker dupes an "innocent" third party to harass.

Similar to North Carolina's cyberstalking statute Louisiana has a model statute, but it is not explicitly clear whether it applies when a cyberstalker dupes an "innocent" third party to harass.

1. Requires a threat.
2. May only apply to direct contact with the victim (e-mail), not other Internet postings.
3. May not apply when a cyberstalker dupes an "innocent" third party to harass.

1. Only applies to direct contact with the victim (e-mail), not other Internet postings.
2. May not apply when a cyberstalker dupes an "innocent" third party to harass.
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Title</td>
<td>Stalking</td>
<td>Stalking</td>
<td>Criminal Harassment</td>
<td>Harassment</td>
<td>Stalking (misdemeanor)</td>
</tr>
<tr>
<td>Reasonable Person Standard?</td>
<td>Yes</td>
<td>No, but has broad standard that covers the intent “to harass”</td>
<td>Yes, but requires a threat</td>
<td>Yes</td>
<td>Stalking (misdemeanor)</td>
</tr>
<tr>
<td>Credible Threat Standard?</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Requires Actual Physical Pursuit?</td>
<td>Yes Approaching or pursuing another</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Statute Covers Electronic Communications?</td>
<td>No</td>
<td>Unclear</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Notes</td>
<td>Requires that stalker be warned/asked to stop conduct</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Potential Statutory Problems

1. Electronic communications are not explicitly covered.
2. Requires physical pursuit, which would not include many aspects of cyberstalking.
3. May not apply when a cyberstalker dupes an "innocent" third party to harass.

1. Electronic communications are not explicitly covered.
2. May not apply when a cyberstalker dupes an "innocent" third party to harass.
3. Requires a threat.
4. May only apply to direct "contact" with the victim (e-mail), not other Internet postings.

1. May only apply to direct "contact" with the victim (e-mail), not other Internet postings.
2. May not apply when a cyberstalker dupes an "innocent" third party to harass.

Code

Minnesota

Mississippi

Mississippi
MISS. CODE ANN. § 97-3-85, 97-29-45 (2000).

Mississippi

Mississippi

Missouri

Montana

Title
Harassment  —  Stalking

Stalking

Reasonable Person Standard?
No

Actor knows or has reason to know it would cause victim under the circumstances to feel fear,
sometimes "credible threat"

Yes

Yes, for stalking

Yes, plus credible threat for aggravated stalking
<table>
<thead>
<tr>
<th>Credible Threat Standard?</th>
<th>and actually causes fear</th>
<th>Requires Actual Physical Pursuit?</th>
<th>Statute Covers Electronic Communications?</th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>Sometimes No</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>Any person who willfully, maliciously, and repeatedly follows or harasses another person, or makes a credible threat, with the intent to place that person in reasonable fear of death or injury</td>
<td>No</td>
<td>Unclear</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Electronic communication has to be received by a person with a unique address</td>
</tr>
</tbody>
</table>
1. May only apply to direct contact with the victim (e-mail), not other Internet postings.
2. May not apply when a cyber-stalker duplicates an "innocent" third party to harass.

Electronic communications are not explicitly covered.
May only apply to direct contact with the victim (email), not other Internet postings.
May not apply when a cyber-stalker duplicates an "innocent" third party to harass.
May not apply when a cyber-stalker duplicates an "innocent" third party to harass.
May not apply when a cyber-stalker duplicates an "innocent" third party to harass.
<table>
<thead>
<tr>
<th>Credible Threat Standard?</th>
<th>Sometimes use of obscene or lewd language or a threat</th>
<th>No</th>
<th>No (Stalking)</th>
<th>Yes</th>
<th>Aggravated Stalking</th>
<th>Yes</th>
<th>No</th>
</tr>
</thead>
<tbody>
<tr>
<td>Requires Actual Physical Pursuit?</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Statute Covers Electronic Communications?</td>
<td>Yes</td>
<td>Unclear</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Notes**

"Person who commits stalking using Internet . . . to publish, display, or distribute information in a manner that substantially increases the risk of harm or violence to the victim." § 200.575(3)

This statute may apply cyberstalker dupes an "innocent" third party to harass and would make it a felony charge. See § 200.575(3)

**Potential Statutory Problems**

1. May only apply to direct contact with the victim (e-mail), not

1. May only apply to direct contact with the victim (e-mail), not

1. Requires a threat.

2. May not apply to

1. May not apply to

2. May not apply to

1. Requires a threat.
other Internet postings.
2. May not apply when a cyberstalker dupes an “innocent” third party to harass.

mail), not other Internet postings.
2. May not apply when a cyberstalker dupes an “innocent” third party to harass.

statute may apply to most aspects of cyberstalking.
3. May not apply when a cyberstalker dupes an “innocent” third party to harass.

third party to harass.
[Note, N.H. harassment statute held unconstitutional.

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Title</td>
<td>Stalking</td>
<td>Stalking</td>
<td>Harassment</td>
<td>Harassment</td>
<td>Harassment</td>
<td>Harassment</td>
</tr>
<tr>
<td>Reasonable Person Standard?</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Credible Threat Standard?</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Requires Actual Physical Pursuit?</td>
<td>Sometimes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>----------------------------------</td>
<td>-----------</td>
<td>----</td>
<td>----</td>
<td>----</td>
<td>----</td>
<td>----</td>
</tr>
<tr>
<td>Either maintain physical proximity or threaten</td>
<td>Not specifically</td>
<td>Not specifically</td>
<td>Not specifically</td>
<td>Not specifically</td>
<td>Not specifically</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Statute Covers Electronic Communications?**

**Notes**

**Potential Statutory Problems**

1. Requires a threat or physical proximity.
2. May not apply to electronic communications.
3. May only apply to direct contact with the victim (e-mail), not other Internet postings.
4. May not apply when a cyberstalker dupes an "innocent" third party to harass.

1. May not apply when a cyberstalker dupes an "innocent" third party to harass.
2. May not apply when a cyberstalker dupes an "innocent" third party to harass.

1. May not apply to electronic communications.
2. May not apply when a cyberstalker dupes an "innocent" third party to harass.

1. May not apply when a cyberstalker dupes an "innocent" third party to harass.
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Title</td>
<td></td>
<td></td>
<td>Stalking</td>
<td>Cyberstalking</td>
<td></td>
</tr>
<tr>
<td>Reasonable Person Standard?</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Credible Threat Standard?</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Requires Actual Physical Pursuit?</td>
<td>No</td>
<td>Yes, must display a weapon</td>
<td>Yes, must cause physical injury</td>
<td>Sometimes</td>
<td>No</td>
</tr>
<tr>
<td>Statute Covers Electronic Communications?</td>
<td>Likely</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Notes</td>
<td></td>
<td></td>
<td></td>
<td>Similar to Louisiana's cyberstalking statute</td>
<td></td>
</tr>
<tr>
<td>Potential Statutory Problems</td>
<td>Code</td>
<td>Title</td>
<td>Reasonable Person Standard?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>-----------------------------</td>
<td>------</td>
<td>-------</td>
<td>-----------------------------</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3. May not apply when a cyberstalker dupes an “innocent” third party to harass.</td>
<td>Ohio OHIO REV. CODE ANN. § 2903.211 (LexisNexis 2006).</td>
<td>Menacing by Stalking</td>
<td>Similar standard (conduct that would “cause another person to believe that the offender will cause physical</td>
<td></td>
<td></td>
</tr>
<tr>
<td>1. Requires physical display of weapon.</td>
<td>Ohio OHIO REV. CODE ANN. § 2917.21 (LexisNexis 2006).</td>
<td>Telecommunications Harassment</td>
<td>No, but uses broad standard that covers the intent “to harass”</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3. May not apply when a cyberstalker dupes an “innocent” third party to harass.</td>
<td>North Carolina has a model statute, but it is not explicitly clear whether it applies when a cyberstalker dupes an “innocent” third party to harass.</td>
<td>Computer Crimes Act (misdemeanor)</td>
<td>No, but uses broad standard that covers the intent “to harass”</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Credible Threat Standard?
- **No**
- **Yes**

### Requires Actual Physical Pursuit?
- **No**

### Statute Covers Electronic Communications?
- **Not specifically**
- **Yes**

### Potential Statutory Problems
1. **May not** apply to electronic communications.
2. **May not** apply when a cyberstalker dupes an “innocent” third party.
3. **May not** apply when a cyberstalker dupes an “innocent” third party to harass.

### Although not explicitly entitled a cyberstalking statute, Ohio has a model statute, particularly because it is one of the few that explicitly addresses “innocent” third party harassers.

### Goodno: Cyberstalking, a New Crime

1. **May not** apply when a cyberstalker dupes an “innocent” third party to harass.

### § 2903.211(A)(1).

### § 2913.01 (LexisNexis 2006).

### See OHIO REV. CODE ANN. § 2903.211(A)(2)(b).

### No

### No

### No

### No
to harass. apply when a cyberstalker dupes an "innocent" third party to harass.

2903.211(A)(2) ("No person, through the use of any electronic method of remotely transferring information, including, but not limited to, any computer, computer network, computer program, or computer system, shall post a message with purpose to urge or incite another to commit a violation of division (A)(1) of this section." (emphasis added).

<table>
<thead>
<tr>
<th>Oregon</th>
<th>Oregon</th>
<th>Pennsylvania</th>
<th>Rhode Island</th>
<th>Rhode Island</th>
<th>South Carolina</th>
</tr>
</thead>
<tbody>
<tr>
<td>Title Stalking</td>
<td>Harassment</td>
<td>Stalking</td>
<td>Stalking</td>
<td>Cyberstalking</td>
<td>Harassment Stalking</td>
</tr>
<tr>
<td>Reasonable Person Standard?</td>
<td>Yes, but requires direct contact</td>
<td>Yes</td>
<td>No, but has broad harassment standard</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>-----------------------------</td>
<td>---------------------------------</td>
<td>-----</td>
<td>--------------------------------------</td>
<td>-----</td>
<td></td>
</tr>
<tr>
<td>Credible Threat Standard?</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td></td>
<td>statutory provisions make it clear that threat or its equivalent must have been made for crime of stalking to be found. See State v. Shields, 56 P.3d 937 (Or. Ct. App. 2002); State v. Rangel, 934 P.2d 1128 (Or. Ct. App. 1997).</td>
<td>No</td>
<td>No</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Requires Actual Physical Pursuit?</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Yes, physical No following when reasonable person standard is used. § 11-59-2(a)(2).</td>
<td>No</td>
<td>No</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Statute</td>
<td>Covers</td>
<td>Electronic Communications?</td>
<td>Potential Statutory Problems</td>
<td></td>
<td></td>
</tr>
<tr>
<td>---------</td>
<td>--------</td>
<td>-----------------------------</td>
<td>-----------------------------</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Yes</td>
<td>See OR. REV. STAT. § 163.730 (2003).</td>
<td>Yes</td>
<td>1. May only apply to direct contact with the victim (e-mail), not other Internet postings. 2. May not apply when a cyberstalker dupes an “innocent” third party to harass.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

1. Requires threat. 2. May only apply to direct contact with the victim (e-mail), not other Internet postings. 3. May not apply when a cyberstalker dupes an “innocent” third party to harass.

1. May only apply to direct contact with the victim (e-mail), not other Internet postings. 2. May not apply when a cyberstalker dupes an “innocent” third party to harass.

1. May not apply when a cyberstalker dupes an “innocent” third party to harass. Rhode Island has a model statute, particularly because it is one of the few that explicitly addresses “innocent” third party harassers. See § 11-52-4.2(a) (“Whoever transmits any communication by computer to any person or causes any person to be contacted for the sole purpose of harassing that person or his or her family is guilty . . . .”)(emphasis added). Yes, for 2nd Deg. Harassment (misdemeanor) 1. May not apply when a cyberstalker dupes an “innocent” third party to harass. |
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Title</td>
<td>Stalking</td>
<td>Harassment</td>
<td>Yes (one option; see “reasonable person standard”)</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Reasonable Person Standard?</td>
<td>Yes, but requires threat; also has broad harassment standard</td>
<td>No (Stalking)</td>
<td>Yes (Aggravated Stalking)</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Credible Threat Standard?</td>
<td>Yes</td>
<td>No (Stalking)</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Requires Actual Physical Pursuit?</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Statute Covers Electronic Communications?</td>
<td>Yes</td>
<td>Yes</td>
<td>Not specifically</td>
<td>Yes</td>
<td>Not specifically</td>
<td>Not specifically</td>
</tr>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Non-consensual contact includes sending electronic communications</td>
<td>Yes</td>
<td>Electronic communication includes a communication initiated by e-mail or instant message</td>
<td></td>
</tr>
</tbody>
</table>
Notes

Potential Statutory Problems

1. May require threat.
2. May not apply when a cyberstalker dupes an “innocent” third party to harass.

1. May only apply to direct contact with the victim (e-mail), not other Internet postings.
2. May not apply when a cyberstalker dupes an “innocent” third party to harass.

1. Requires threat.
2. May only apply to direct contact with the victim (e-mail), not other Internet postings.
3. May not apply when a cyberstalker dupes an “innocent” third party to harass.

Statute requires either an obscene proposal or threat

1. Requires a threat.
2. May not apply to electronic communications.
3. May not apply when a cyberstalker dupes an “innocent” third party to harass.

1. May not apply to electronic communications.
2. May not apply when a cyberstalker dupes an “innocent” third party to harass.
3. May not apply when a cyberstalker dupes an “innocent” third party to harass.
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Title</td>
<td>Stalking</td>
<td>Electronic Communication Harassment</td>
<td>Stalking</td>
<td>Disturbing Peace by Use of Electronic Communication (misdemeanor)</td>
<td>Harassment by Computer (misdemeanor)</td>
</tr>
<tr>
<td>Reasonable Person Standard?</td>
<td>Yes, but requires a threat</td>
<td>No, but has standard where stalker insults, taunts, or challenges the recipient in a manner likely to provoke a violent or disorderly response</td>
<td>Yes</td>
<td>Yes (one option; see “reasonable person standard”)</td>
<td>No</td>
</tr>
<tr>
<td>Credible Threat Standard?</td>
<td>Yes visual or physical proximity to a person, or threats</td>
<td>No</td>
<td>Yes</td>
<td>Yes (one option; see “reasonable person standard”)</td>
<td>No</td>
</tr>
<tr>
<td>Requires Actual Physical Pursuit?</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Statute Covers Electronic Communication</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>
Potential Statutory Problems

1. May require a threat.
2. May only apply to direct contact with the victim (e-mail), not other Internet postings.
3. May not apply when a cyberstalker dupes an “innocent” third party to harass.

1. There are potential constitutional issues with this statute. See, e.g., Provo City Corp. v. Thompson, 86 P.3d 735 (Utah 2004).
2. May only apply to direct contact with the victim (e-mail), not other Internet postings.
3. May not apply when a cyberstalker dupes an “innocent” third party to harass.

Also prevents conduct that causes disruption, jamming, or overload of an electronic communication system through excessive message traffic of other means utilizing communication device.

1. May only apply to direct contact with the victim (e-mail), not other Internet postings.
2. May not apply when a cyberstalker dupes an “innocent” third party to harass.

May address e-mail bombs. See § 13-1027(a)(ii).

May cover “innocent” third party harassers. “Use [of] a computer . . . to communicate obscene, vulgar, profane, lewd, lascivious, or indecent language, or make any suggestion or proposal of an obscene nature.” § 18.2-152.7:1.

If “innocent” third party harassers are covered by this statute, then it may cover most aspects of cyberstalking; however, it is written so broadly that it may create constitutional issues.
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Virginia</td>
<td>Stalking</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>May cover e-mail bombs. See § 9.61.260(1)(b).</td>
</tr>
<tr>
<td>VA. CODE ANN.</td>
<td>WASH. REV. CODE § 9.61.260 (Supp. 2004). Cyberstalking</td>
<td>No, but has broad harassment standard Yes (one option; see “reasonable person standard”)</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td></td>
<td>WASH. REV. CODE § 9A.46.110 (2000 &amp; Supp. 2006). Stalking</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes (one option; see “reasonable person standard”)</td>
</tr>
<tr>
<td></td>
<td>WASH. REV. CODE § 9.61.230 (2003). Telephone Harassment</td>
<td>No, but has broad harassment standard Yes (one option; see “reasonable person standard”)</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td></td>
</tr>
</tbody>
</table>

Goodno: Goodno: Cyberstalking, a New Crime
Potential Statutory Problems

1. May not apply when a cyberstalker dupes an “innocent” third party to harass.

Washington has a model statute, particularly because it is one of the few that explicitly addresses “innocent” third party harassers. See § 9.61.260(1)(a) (“A person is guilty of cyberstalking if he or she . . . makes an electronic communication to such other person or a third party. . . . Using any lewd, lascivious, indecent, or obscene words, images, or language, or suggesting the commission of any lewd or lascivious act.”) (emphasis added).

1. Statute has been held unconstitutional. See State v. Williams, 26 P.3d 890 (Wash. 2001).
2. Requires threat.
3. May not apply when a cyberstalker dupes an “innocent” third party to harass.

1. Does not apply to electronic communications (limited only to telephone communications).
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Title</td>
<td>Stalking Harassment</td>
<td>Threatening Communications by Computer</td>
<td>Stalking Harassment</td>
<td>Harassment</td>
<td>Unlawful use of computerized communication systems (misdemeanor)</td>
</tr>
<tr>
<td>Reasonable Person Standard?</td>
<td>Yes See § 61-2-9a(g)(1)</td>
<td>No, uses broad harassment standard, but requires cyber-stalker to contact victim</td>
<td>Yes, but requires direct contact with victim</td>
<td>No, but uses broad harassment standard</td>
<td>No, but uses broad harassment standard</td>
</tr>
<tr>
<td>Credible Threat Standard?</td>
<td>Yes (one option; see “physical pursuit”)</td>
<td>Yes (one option)</td>
<td>Yes (one option; see “reasonable person standard”)</td>
<td>Yes (one option; see “reasonable person standard”)</td>
<td></td>
</tr>
<tr>
<td>Requires Actual Physical Pursuit?</td>
<td>Sometimes Requires following unless there is repeated harassing or credible threats</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Statute Covers Electronic Communications?</td>
<td>Yes</td>
<td>Not specifically, but course of conduct includes sending material by any means to the victim</td>
<td>Not specifically</td>
<td>Yes</td>
<td>193</td>
</tr>
</tbody>
</table>
Notes
Potential Statutory Problems

1. May not apply to electronic communications.
2. May not apply when a cyberstalker dupes an “innocent” third party to harass.

1. May only apply to direct contact with the victim (e-mail), not other Internet postings.
2. May not apply when a cyberstalker dupes an “innocent” third party to harass.

1. May not apply to electronic communications.
2. May only apply to direct contact with the victim (e-mail), not other Internet postings.
3. May not apply when a cyberstalker dupes an “innocent” third party to harass.

1. May not apply to electronic communications.
2. May only apply directly to the victim (e-mail), not other Internet postings.
2. May not apply when a cyberstalker dupes an “innocent” third party to harass.

Code

Wyoming

Title
Stalking

Reasonable Person Standard?
Yes, but may require a threat. See § 6-2-506(a)(ii).

Credible Threat Standard?
Yes. See § 6-2-506(a)(ii).

Requires Actual Physical Pursuit?
No
Statute Covers Electronic Communications?

Notes

Potential Statutory Problems

1. May require a threat.
2. May only apply to direct contact with the victim (e-mail), not other Internet postings.
3. May not apply when a cyberstalker dupes an "innocent" third party to harass.
## APPENDIX: FEDERAL CODES

<table>
<thead>
<tr>
<th>Code</th>
<th>FEDERAL CODE</th>
<th>FEDERAL CODE</th>
<th>FEDERAL CODE</th>
</tr>
</thead>
</table>

| Reasonable Person Standard? | No | No, but has broad harassment standard | Yes |
| Credible Threat Standard? | Yes | No | No |
| Requires Actual Physical Pursuit? | No | No | No |

| Statute Covers Electronic Communications? | Yes | Yes |  |

| Notes | 1. Requires a threat. 2. May only apply to direct contact with the victim (e-mail), not other Internet postings. 3. May not apply when a cyberstalker dupes an “innocent” |
| Potential Statutory Problems | 1. Requires messages to be anonymously sent. 2. May only apply to direct contact with the victim (e-mail), not other Internet postings. 3. May not apply | 1. May not apply when a cyberstalker dupes an “innocent” third party to harass. |
when a cyberstalker dupes an "innocent" third party to harass.