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

Naomi Harlin Goodno[a]

Introduction

The Internet is a powerful and wonderful tool that has brought on a new information age. If it is purposely misused, however, it 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 calls day or night at [current telephone number] . . . I promise you everything you 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 just 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":

---

[a] 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, and Judge Tim Tymkovich of the Tenth Circuit for their 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.

[1] J.A. HITCHCOCK, NET CRIMES AND MISDEMEANORS: OUTMANEUVERING THE SPAMMERS, SWINDLERS, AND STALKERS WHO ARE TARGETING YOU ONLINE 11 (2002).

[2] HITCHCOCK, *supra* note 1, at 23.

"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]

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 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] "There link between cyberstalking and the sexual abuse of children is also recognized by the U.S. government."[9]

---

[3] HITCHCOCK, *supra* note 1, at 112.
[4] U.S. Department of Justice, *Stalking and Domestic Violence: Report to Congress*, 1 (May 2001), 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.
[5] Renee L. Servance, *Cyberbullying, Cyber-Harassment, and the Conflict Between Schools and the First Amendment*, 2003 WIS. L. REV. 1213, 1215 (2003).
[6] Patricia Tjaden & Nancy Thoennes, *Stalking in America: Findings From the National Violence Against Women Survey*, 1 (National Institute of Justice & Center for Disease Control and Prevention) (1998). ("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. . . . 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 6.
[8] *Report to Congress*, *supra* note 4, at 6.
[9] PAUL BOCIJ, CYBERSTALKING: HARASSMENT IN THE INTERNET AGE AND HOW TO PROTECT YOUR FAMILY 11 (2004).

This article explores why the nature of cyberstalking represents a form of behavior that is distinct from "offline stalking"[10] such that the interpretation of many of the statutes dealing with offline stalking may be inadequate to address the problem.[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 and deal with potential 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.

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.[12]

I. Cyberstalking vs. Offline Stalking

a. Brief Review of Offline Stalking

While cyberstalking is as recent a phenomena as the Internet itself, even offline

[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.

[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." http://en.wikipedia.org/wiki/Cyberstalking.

[12] *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.

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.[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*. 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.[14]

Other states, and soon the federal government, followed California's lead and enacted stalking statutes to "fill gaps in the law."[15] Legislatures importantly recognized the need to stop stalkers before the stalking developed "into a more serious threat to a victim's personal safety."[16] Additionally, stalking laws were enacted "to eliminate behaviors which disrupt normal life for the victim, and to prevent such behaviors from escalating into violence."[17] 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."[18]

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. [19] Offline stalking has "a profound effect upon the victim" by causing post-traumatic stress

---

[13] *See id. at 120-25.*
[14] Wayne R. LaFave, *Physical Harm and Apprehension Thereof*, *in* SUBSTANTIVE CRIMINAL LAW CURRENT THROUGH THE 2006 UPDATE, PART THREE — OFFENSES AGAINST THE PERSON, 2 Subst. Crim. L. § 16.4(b) Stalking (2d ed. 2006) [hereinafter *Physical Harm and Apprehension Thereof*].
[15] Curry v. State, 811 So. 2d 736, 741 (Fla. Dist. Ct. App. 2002).
[16] *Id.* at 743.
[17] James Thomas Tucker, *Stalking the Problems With Stalking Laws: The Effectiveness of Florida Statutes Section 784.048*, 45 FLA. L. REV. 609, 617 (1993).
[18] *Id.* Cyberstalking statutes should reflect the same goals of being proactive and preventative.
[19] *Physical Harm and Apprehension Thereof*, *supra* note ____.

disorder, depression[20] and serious emotional distress, and also by escalating to physical attacks. 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.[21] Similarities that are pointed to include: a desire to exert control over the victim;[22] and, much like offline stalking, cyberstalking involves repeated harassing or threatening behavior, which is often a prelude to more serious behavior.[23] While these similarities do exist, cyberstalking differs from offline stalking in four important ways. These differences are crucial because they are the reasons why offline 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. 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, Internet 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

[20] *Physical Harm and Apprehension Thereof*, *supra* note ____.
[21] Servance, *supra* note ____, at 1219.
[22] *Report to Congress*, *supra* note ____, at 1.
[23] *Report to Congress*, *supra* note ____, at 1; Harry Valetk, *Mastering the Dark Arts of Cyberspace: A Quest for Sound Internet Safety Policies*, 2004 STAN. TECH. L. REV. 2, 54 (2004).

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").[24]

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.[25]

2. Cyberstalkers can be physically far removed from their victim. Offline stalking often entails situations where the stalker is physically near the victim (i.e., in the same geographical area).[26] Cyberstalkers, however, can use the Internet to terrify their victim no matter where in the world she is; thus, she 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

[24] BOCIJ, *supra* note ___ at 2.
[25] HITCHCOCK, *supra* note ____, at 100-116.
[26] *Report to Congress*, *supra* note ____, at 3; Valetk, *supra* note ____, at 54.

likely cheaper to use 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.[27] 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.

3. Cyberstalkers can remain nearly anonymous.[28] There is a common misperception that cyberstalking is less dangerous than offline stalking because it does not involve physical contact.[29] The opposite, however, 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 a harassing or threatening electronic communication.[30]

The environment of cyberspace is designed to allow 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. Perpetrators may even

---

[27] *See, e.g.,* Louse Ellison, *Cyberstalking: Tackling Harassment on the Internet, in* CRIME AND THE INTERNET (David S. Wall ed., 2001).

[28] 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. 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.). Where the courts and history have recognized a free speech value to anonymity, it has almost always meant pseudo-anonymity. 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.

[29] Neal Kumar Katyal, *Criminal Law in Cyberspace*, U. PA. L. REV. 1003 (2001).

[30] *See* BOCIJ, *supra* note ____, at 90-106.

be encouraged to continue these acts.[31] 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.[32]

As one scholar has explained, there is a "veil of anonymity" on the Internet that puts cyberstalkers "at an advantage."[33] 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. [34]

4. Cyberstalkers can easily impersonate the victim. Unlike offline stalking, the cyberstalker can easily take on the identity of the victim and create havoc on-line. The cyberstalker, pretending to be the victim, 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. [35] Moreover, for over a year, the cyberstalker "e-mail bomb[ed]" her by

---

[31] *Report to Congress*, *supra* note ____, at 2.
[32] Such conduct would still be considered harassment if the cyberstalker has the intent to harass the victim. *See* U.S. Department of Justice, *1999 Report on Cyberstalking: A New Challenge for Law Enforcement and Industry — A Report From the Attorney General to the Vice President,* 12 (Aug. 1999), http://www.usdoj.gov/criminal/cybercrime/cyberstalking.htm (last visited Aug. 2005)[hereinafter *1999 Report on Cyberstalking*].
[33] Amy C. Radosevich, Note, *Thwarting the Stalker: Are Anti-Stalking Measures Keeping Pace with Today's Stalkers?*, 2000 U. ILL. L. REV. 1371, 1387 (2000).
[34] Radosevich, *supra* note ____, at 1388.
[35] 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

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."[36] The cyberstalker's actions became so unbearable that Hitchcock was forced to physically move, but that did not stop him. He eventually found her on-line and would begin to harass her again. Hitchcock sued him,[37] but the cyberstalker was never held criminally liable.[38]

5. Cyberstalkers can encourage "innocent" third-party harassment.[39]

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.[40] 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.[41] Hitchcock experienced a similar form of

---

festering away your small brains. I may or may not resign. I may stay to awaken you idiots . . . ." HITCHCOCK, *supra* note ____, at 8.

[36] HITCHCOCK, *supra* note ____, at 5-14.

[37] *Id. See also* BOCIJ, *supra* note ____, at 1-3.

[38] Hitchcock sued her cyberstalker who eventually settled. The cyberstalker also pled guilty to conspiracy to commit mail fraud and perjury for the conduct related to Hitchcock's original complaints. However, he was never prosecuted for any crime related to stalking or harassment. BOCIJ, *supra* note ____, at 2.

[39] Other scholars have referred to this as "stalking by-proxy." *See* BOCIJ, *supra* note ____, at 25-26.

[40] *See* Bill Wallace, *Stalkers Find a New Tool -- The Internet E-mail Is Increasingly Used to Threaten and Harass, Authorities Say,* S.F. CHRONICLE, Jul. 10, 2000, available at http://www.sfgate.com/cgi-bin/article.cgi?file=/chronicle/archive/2000/07/10/MN39633.DTL.

[41] *See id.*

cyberstalking when her cyberstalker advertised her telephone and address on an alt-sex site advertising for "sadistic interaction."[42]

Another example of duping "innocent" third parties to do the harassing involves a cyberstalker that sent hate e-mail in his victim's name, often times with her telephone number and address, "to groups of Satanist, drug users and pornographers."[43] 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: "'You'd better get a gun because the next time we read about you it will be in a police report.'"[44] It was later discovered that the cyberstalker was the victim's disgruntled business acquaintance, but the victim had no criminal recourse.[45]

In the end, 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.[46]

---

[42] HITCHCOCK, *supra* note ____, at 11.
[43] N.Y. State Assemb. A05376 (N.Y. 2006), *available at* http://assembly.state.ny.us/leg/?bn=A05376.
[44] *Id.*
[45] *Id.*
[46] *See, e.g.,* Radosevich, *supra* note ____, 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 forces; combating technology with technology by providing computerized response systems for victims; launching public awareness campaigns and educational Websites so that victims are informed of their options and rights; and getting Internet Service Providers involved in the regulation process. *Id.* at 1391-95.

II. 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.[47] 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.[48]

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

[47] *See infra* Appendix to this article.
[48] Because stalking statutes are all over the board, this next section is not intended to summarize all harassment laws. However, it does attempt to generally categorize the statutes to determine what requirements are most adequate to combat cyberstalking.

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.[49] 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.[50] Although there are many differences in offline stalking statutes, the majority of them have a similar intentional mental state requirement.[51]

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.[52] 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

---

[49] *See, e.g.,* United States v. Apfelbaum, 445 U.S. 115, 131 (1980); JOSHUA DRESSLER, CASES AND MATERIALS ON CRIMINAL LAW 121 (3d ed. 2003) (specifying that crimes conventionally have both elements).

[50] *See infra* Appendix to this article. *See, e.g.*, ALA. CODE § 13A-6-90 (2005) ("Stalking" requires that a person intentionally follow or harass another person, and intend to place this other person in reasonable fear of death or serious bodily harm.). ARIZ. REV. STAT. ANN. § 13-2923 (2005) ("A person commits stalking if the person intentionally or knowingly engages in a course of conduct that is directed toward another person, and if that conduct" would cause a reasonable person fear.); LA. REV. STAT. ANN. § 14:40.2 (2005) ("Stalking is the intentional and repeated following or harassing of another person that would cause a reasonable person to feel fear…."). *But see* ALASKA STAT. §§ 11.41.260- 41.270 (2004) (requiring only that the perpetrator "knowingly" engage in a course of conduct that recklessly places another person in fear of death or physical injury).

[51] *See infra* Appendix to this article.

[52] *See id.*

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.[53] 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.

The second consideration, however, 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,[54] there are three different types of conduct that offline stalking statutes criminalize: (1) conduct requiring an element of physical or visible proximity to the victim;[55] (2) conduct conveying verbal or written threats or threats implied by conduct, i.e., a "credible threat";[56] and (3) conduct that would cause a "reasonable person" to fear physical harm or to suffer severe emotional distress (hereinafter the "reasonable person standard").[57] 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

---

[53] *See, e.g.*, ARK. CODE ANN. § 5-71-229 (West 2005) (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 to this article.

[54] 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.

[55] ARIZ. REV. STAT. ANN. § 13-2923 (2005).

[56] *See, e.g.*, ALASKA STAT. § 11.61.120(a)(4) (2004); *see also infra* Appendix to this article.

[57] *See, e.g,* ARIZ. REV. STAT. ANN. § 13-2921 (2005); CAL. PENAL CODE § 646.9 (West 2005); CONN. GEN. STAT. ANN. § 53a-181e (West 2005); IDAHO CODE ANN. §§ 18-7905 to -7906 (2005); MINN. STAT. ANN. § 609.749 (West 2005); *see also infra* Appendix to this article.

person" standard can fully address cyberstalking because such laws correctly focus on the effect of the perpetrator's conduct on the victim (e.g., the fear felt by the victim).[58]

(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.[59] Since the very nature of cyberstalking allows the cyberstalker to be in an entirely different physical location than 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.[60] Under Georgia's stalking statute at that time (the statute has since been amended), [61] the cyberstalker was found innocent of stalking because his conduct did not include the physical pursuit of the victim.[62]

(ii) Problems with credible threat requirement. Many current stalking statutes require the perpetrator to make a "credible threat" of violence against the victim.[63] Generally, a credible threat is "a verbal or written *threat*" coupled "with the *apparent*

---

[58] Joseph C. Merschman, *The Dark Side of the Web: Cyberstalking and the Need for Contemporary Legislation*, 24 HARV. WOMEN'S L.J. 255, 260 (2001).
[59] *See, e.g,* CONN. GEN. STAT. ANN. § 53a-181c (West 2005); IOWA CODE ANN. § 708.11 (West 2005); MD. CODE ANN., CRIM. LAW § 3-802 (West 2005) (formerly MD. ANN. CODE art. 27, § 124); N.J. STAT. ANN. § 2C:12-10 (West 2005); N.C. GEN. STAT. ANN. § 14-277.3 (West 2005); UTAH CODE ANN. § 76-5-106.5 (West 2005); WYO. STAT. ANN. § 6-2-506 (2005); *see also infra* Appendix to this article.
[60] *See Working to Stop Online Abuse,* http://www.cyberstalked.org/ourstory.
[61] GA CODE ANN. § 46-5-21 (West 2006).
[62] *See Working to Stop Online Abuse,* http://www.cyberstalked.org/ourstory.
[63] Over one-third of state stalking statutes have a credible threat requirement. *See infra* Appendix to this article; *see also Report to Congress*, *supra* note ____, at 1.

ability to carry out the threat" so as to cause the victim fear.[64] 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 punishment of 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."[65]

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.[66]

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-issues which become even more acute in cyberstalking cases.[67] In *Iowa v. Limbrecht*,[68] 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

---

[64] CAL. PENAL CODE § 646.9 (West 2006) (emphasis added).
[65] Merschman, *supra* note ___ at 260.
[66] *See, e.g.*, CAL. PENAL CODE § 646.9 (West 2005) (harassing electronic communications do not constitute cyberstalking unless there is a credible threat). *See* Iowa v. Limbrecht, 600 N.W.2d 316 (Iowa 1999); United States v. Alkabazah, 104 F.3d 1492 (6th Cir. 1997).
[67] *Compare* IOWA CODE § 780.11 (1993), *with* IOWA CODE § 780.11 (2006).
[68] *Limbrecht*, 600 N.W.2d at 316-17.

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.[69] 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.[70] The defendant also drove by Corey's house a number of times, which ultimately led to his arrest and stalking conviction.[71] The defendant appealed his conviction arguing that he never explicitly threatened to hurt Corey. The court acknowledged that the defendant never threatened Corey, 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.[72] 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.[73]

As exemplified by *Limbrecht*, the issue of whether a credible threat requirement is the appropriate standard is being debated in offline stalking cases.[74] This issue, however,

---

[69] *Limbrecht*, 600 N.W.2d at 317.
[70] *Id.* at 318-19.
[71] *Id.* at 319.
[72] *Id. See also* IOWA CODE ANN. § 708.11(1)(a) (West 1993) (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.").
[73] *Limbrecht*, 600 N.W.2d at 319 (citing IOWA CODE § 708.11(1)(b) (1997)). *See also* 1994 IOWA ACTS 1093, § 4.
[74] 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 ____, 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.").

is even more acute with cyberstalking.[75] 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.[76] Cyberstalkers, on the other hand, can easily use the Internet to send hundreds, even thousands, of frightening e-mail messages (similar the letters sent in *Limbrecht*) in a matter of one hour,[77] which over days and weeks can create havoc on 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. [78]

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 Web pages and blogs. In cyberstalking cases then, the stalker can quickly and effortlessly engage in terrifying conduct to harass the victim—conduct no less threatening than an actual threat—with world-wide dissemination.

---

[75] *Report to Congress*, *supra* note ____, at 45 n.3. *See also* Federal Interstate Stalking Statute, 18 U.S.C. § 2261A (2006) (codifying a "reasonable fear" standard).

[76] *Limbrecht*, 600 N.W.2d at 317-18.

[77] 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.

[78] 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, instant messenger, etc.). *See, e.g.,* KY. REV. STAT. ANN. §§ 508.130-.150 (West 2005); N.M. STAT. ANN. §§ 30-3A-3 to -3A-3.1 (West 2005); N.Y. PENAL LAW § 120.60 (McKinney 2005).

For example, in one case, a cyberstalker created a webpage "dedicated" to his young victim, Amy Boyer.[79] 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.[80] 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 might have been difficult for Boyer to establish that there was a credible threat. A threat was never sent directly to her, so it would have been difficult to show that the cyberstalker actually threatened her.[81]

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.

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

---

[79] HITCHCOCK, *supra* note ____, at 100-116.
[80] *Id.*
[81] *See intra* part III of this article (fully explaining United States v. Alkhabaz, 104 F.3d 1492 (6th Cir. 1997)).

electronic communication. Cyberstalkers covet anonymity because it allows them to hide from reality and from their victims.[82] Victims who are stalked by unknown persons cannot know the perpetrator's habits or intentions.[83] Thus, as 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. Thus, 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.[84] 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—either those that have attempted to incorporate cyberstalking in preexisting statutes or those that have been specifically targeted at cyberstalking—which have a credible threat requirement 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.

---

[82] Rebecca K. Lee, *Romantic and Electronic Stalking in a College Context*, 4 WM. & MARY J. WOMEN & L. 373, 381-82 (1998). Also, because the 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.
[83] Lee, *supra* note ___ at 382.
[84] Rose Hunter, *Cyberstalking*, (2001), http://gsulaw.gsu.edu/lawand/papers/fa01/hunter/.

(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.[85] Such standard has no physical proximity requirement. Furthermore, the standard addresses many of 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 focus is 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.[86] Facially, 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

[85] 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. ANN. § 53a-182b (West 2005); N.D. CENT. CODE § 12.1-17-07 (2005); WASH. REV. CODE ANN. § 9.61.230 (West 2005). *See also infra* Appendix to this article. 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)(1)(A)-(D) (West 2005); CAL. PENAL CODE § 653m (West 2005); CONN. GEN. STAT. ANN. § 53a-183 (West 2005); DEL. CODE ANN. tit. 11, §§ 1311-12 (2005); *see also infra* Appendix to this article.

[86] DEL. CODE ANN. tit. 11, § 1312A (2005).

by conduct (a standard akin to a "credible threat").[87] 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.[88] Currently, only one state has taken the approach to specifically criminalize such behavior.[89] 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.

III. 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. Rather, they are all over the board.[90] 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 which shift the focus from the perpetrator's behavior to the effect on the victim.[91]

---

[87] *Id. See also* IOWA CODE ANN. § 708.11 (West 2005) ("Course of conduct" requires either repeatedly maintaining a visual or physical proximity, or a threat).
[88] *See supra* part I of this article.
[89] OHIO REV. CODE ANN. § 2917.21 (B) (West 2005).
[90] *See infra* Appendix to this article.
[91] Merschman, *supra* note ____, at 255-56.

Generally, there are three categories of state laws.[92] 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.[93] There are other statutes that do not address cyberstalking because it is unclear if they cover any form of electronic communication.[94] For example, some states have a telephone harassment statute, but the statute only covers telephone communications (not specifically electronic communications).[95] Laws that require physical pursuit and laws that fail to include electronic communications cannot reach cyberstalking.

2. Gaps in 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 offline stalking statutes to cover cyberstalking via "electronic communications."[96] The type of electronic communications covered by these statutes varies. While some states simply inserted the

---

[92] 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 to this article.

[93] *See, e.g,* CONN. GEN. STAT. ANN. § 53a-181 (West 2005); MD. CODE ANN., CRIM. LAW § 3-802 (West 2005) (formerly MD. ANN. CODE art. 27, § 124); IOWA CODE ANN. § 708.11 (West 2005); N.Y. PENAL LAW § 120.55 (McKinney 2005); N.Y. PENAL LAW § 120.60 (McKinney 2005); *see also infra* Appendix to this article.

[94] *See, e.g,* ARK. CODE ANN. § 5-71-229 (West 2005); CONN. GEN. STAT. ANN. § 53a-181e (West 2005); D.C. CODE § 22-404 (2005); *see also infra* Appendix to this article.

[95] *See, e.g.,* KAN. STAT. ANN. § 21-4113 (West 2005); GA. CODE ANN. § 16-5-96 (West 2005).

[96] *See, e.g.*, GA. CODE ANN. § 16-5-90 (West 2005) ("contact" means "any communication including but not limited to communication by computer, computer network, or by any other electronic device."); HAW. REV. STAT. ANN. §§ 711-1106.4 to -1106.5 (LexisNexis 2005) (non-consensual contact includes contact via electronic mail transmission).

general phrase "electronic communications" into existing statutes, others identified specific types of communications (e.g., e-mails, computer communications, or communications on the network).[97] Although it is 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,[98] but state legislatures have introduced bills targeted specifically at cyberstalking and at making it a felony.[99] 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.[100] Such statutes may unnecessarily carve out those

---

[97] *See, e.g., infra* Appendix to this article; CAL. PENAL CODE § 646.9 (West 2005) (including a computer with in the meaning of an "electronic communication device," and defining "electronic communications" according to 18 U.S.C. § 2510(12) (2006)); HAW. REV. STAT. ANN. § 711-1106.4 to -1106.5 (LexisNexis 2005) ("Non-consensual contact" includes contact via electronic mail transmission); GA. CODE ANN. § 16-5-90 (West 2005) (including, but not limiting communication to communication by computer, computer network, or by any other electronic device); *see also*, Shawn Hutton & Sandy Haantz, *Cyberstalking*, (National White Collar Crime Center), 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.

[98] N.Y. PENAL LAW § 240.30 (McKinney 2005); N.Y. PENAL LAW §§ 120.45-50 (McKinney 2005).

[99] N.Y. State Assemb. A05376 (N.Y. 2006), *available at* http://assembly.state.ny.us/leg/?bn=A05376.

[100] *See* MD. CODE ANN., CRIM. LAW § 3-805(a) (West 2005); s*ee also* ALASKA STAT. §§ 11.41.260 to 41.270 (2004); ARK. CODE ANN. § 5-71-209(a)(1) (West 2005); DEL. CODE ANN. tit. 11, § 1312A (2005); ARK. CODE ANN. § 5-41-108(a)(1)(A)-(D) (West 2005); CONN. GEN. STAT. ANN. § 53a-183 (West 2005); CONN. GEN. STAT. ANN. § 53a-182b (West 2005); GA. CODE ANN. § 16-5-90 (West 2005); IDAHO CODE ANN. § 18-7906(2)(a) (2005); IND. CODE ANN. § 35-45-2-2(a)(4)(A)-(B) (West 2005); IOWA CODE ANN. §

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.[101] It also carves out those cases where the cyberstalker encourages "innocent" third party harassment.

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.[102] Other statutes require that the communication contain a credible threat when the perpetrator is not physically pursuing the victim.[103] And, there are even other statutes that, at first glance, seem to have a reasonable person standard, but upon close reading still require that a credible threat be made.[104] 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.

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

---

708.71(a)(1) (West 2005); KY. REV. STAT. ANN. §§ 525.080 (West 2005); TENN. CODE ANN. § 39-17-315 (West 2005); W. VA. CODE ANN. § 61-3C-14a (LexisNexis 2005).

[101] HITCHCOCK, *supra* note ____, at 112.

[102] *See, e.g.,* ARK. CODE ANN. § 5-71-229 (West 2005); FLA. STAT. ANN. § 836.10 (West 2005).

[103] *See, e.g.,* ARIZ. REV. STAT. ANN. § 13-2923 (2005) (requiring an actual threat when the perpetrator is not physically pursuing the victim); ARK. CODE ANN. § 5-71-229 (West 2005) (same); DEL. CODE ANN. tit. 11, § 1312A (2005) (same).

[104] *See, e.g.,* ALA. CODE § 13A-6-90 (2005); CAL. PENAL CODE § 646.9 (West 2005); DEL. CODE ANN. tit. 11, § 1312A (2005); IOWA CODE ANN. § 708.11 (West 2005); ME. REV. STAT. ANN. tit. 17-A, § 210-A(2)(A) (2005); MASS. GEN. LAWS ANN. ch. 265, § 43 (West 2005); N.D. CENT. CODE § 12.1-17-07 (2005); UTAH CODE ANN. § 76-5-106.5 (West 2005); WYO. STAT. ANN. § 6-2-506(a)(ii) (2005); *see also infra* Appendix to this article.

that might address cyberstalking – those directed at stalking and those directed at harassment.[105] Generally, harassment statutes has a broader reach addressing those situations where the stalker engages in conduct with intent to "annoy," "harass," or "alarm" the victim.[106] 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.[107]

3. Gaps in state statutes that are intended to address cyberstalking.

The last category of state laws is comprised of a small group of statutes that specifically deal with cyberstalking. As of August 2006, there are only six states (Illinois, Louisiana, Mississippi, North Carolina, Rhode Island, and Washington) that enacted new "cyberstalking" statutes.[108] 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.[109]

---

[105] *See infra* Appendix to this article.

[106] *See, e.g.,* HAW. REV. STAT. ANN. § 711-1106 (LexisNexis 2005). IND. CODE ANN. § 35-45-10-1, -5(b)(1)(B) (West 2005); IOWA CODE ANN. § 708.7 (West 2005); ME. REV. STAT. ANN. tit. 17-A, § 210-A (2005).

[107] *See, e.g.,* ARK. CODE ANN. § 5-41-108(a)(1)(A)-(D) (West 2005); CAL. PENAL CODE § 653m (West 2005); CONN. GEN. STAT. ANN. § 53a-183 (West 2005); DEL. CODE ANN. tit. 11, §§ 1311-12 (2005); FLA. STAT. ANN. § 784.048 (West 2005); IOWA CODE ANN. § 708.7 (West 2005); KY. REV. STAT. ANN. §§ 525.080 (West 2005); MICH. COMP. LAWS ANN. § 750.411h (West 2005); MO. ANN. STAT. § 565.225 (West 2005); NEV. REV. STAT. ANN. § 200.575 (West 2005); S.C. CODE ANN. § 16-3-1700 (2005).

[108] 720 ILL. COMP. STAT. ANN. 5/12-7.5 (West 2005); LA. REV. STAT. ANN. § 14:40.3 (2005); MISS. CODE ANN. § 97-45-15 (West 2005); N.C. GEN. STAT. ANN. § 14-196.3 (West 2005); R.I. GEN. LAWS § 11-52-4.2 (2004); WASH. REV. CODE ANN. § 9.61.260 (West 2005).

[109] 720 ILL. COMP. STAT. ANN. 135/1-2 (West 2005) (harassment); 720 ILL. COMP. STAT. ANN. 5/12-7.5 (West 2005) (cyberstalking); LA. REV. STAT. ANN. § 14:40.2 (2005) (stalking); LA. REV. STAT. ANN. § 14:40.3 (2005) (cyberstalking); MISS. CODE ANN. § 97-3-107 (West 2005) (stalking with reasonable person standard); MISS. CODE ANN. § 97-45-15 (West 2005) (cyberstalking); N.C. GEN. STAT. ANN. § 14-277.3 (West 2005) (stalking with reasonable person standard); N.C. GEN. STAT. ANN. § 14-196.3 (West 2005) (cyberstalking); R.I. GEN. LAWS §§ 11-59-1 and 2 (2004) (stalking with harassment standard); R.I. GEN. LAWS § 11-52-4.2 (2004) (cyberstalking); WASH. REV. CODE ANN. § 9A.46.110 (West 2005) (stalking

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."[110] This Washington statute also applies to electronic communications.[111] Despite that Washington had a stalking statute with the reasonable person standard that applied to electronic communications, in 2004, the state determined that the best way to deal with cyberstalking was to enact a law specifically addressing it.[112] Other states should follow Washington's example.

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.[113] The Florida Legislature, for example, recognized the dangers of relaxed cyberstalking laws, and amended the Florida stalking statute to provide criminal penalties for "the willful, malicious, and repeated following, harassing, or cyberstalking of another person."[114] By definition, "cyberstalk" means "to engage in a course of conduct to communicate, or to cause to be communicated, words,

---

with a reasonable person standard); WASH. REV. CODE ANN. § 9.61.260 (West 2005) (cyberstalking); W. VA. CODE ANN. § 61-2-9a (LexisNexis 2005) (stalking with reasonable person standard); W. VA. CODE ANN. § 61-3C-14a (LexisNexis 2005) (threatening communications by computer).

[110] WASH. REV. CODE ANN. § 9A.46.110(1)(c)(ii) (West 2005) *amended by* 2006 Wash. Legis. Serv. Page no. 2 (West).

[111] WASH. REV. CODE ANN. § 9A.46.110(2)(b)(4).

[112] WASH. REV. CODE ANN. § 9.61.260 (West 2005).

[113] FLA. STAT. ANN. § 784.048(c)(2)-(3) (West 2005) (stalking statute specifically amended to define the crime of "cyberstalking;" for a misdemeanor charge only, unless coupled with a credible threat); DEL. CODE ANN. tit. 11, §§ 1311-12 (2005) (for a misdemeanor charge only); NEV. REV. STAT. ANN. § 200.575 (West 2005); VA. CODE ANN. § 18.2-152.7:1 (West 2005) (misdemeanor).

[114] FLA. STAT. ANN. § 784.048 (West 2005).

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."[115] 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."[116] To fully address the gaps in state laws, state stalking statutes should be reviewed accordingly.[117]

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.[118] The Illinois cyberstalking statute, for example, does not explicitly address incitement of third party harassment.[119]

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."[120] Likewise, Mississippi's

---

[115] FLA. STAT. ANN. § 784.048(1)(d).
[116] Lopez v. Lopez, 922 So. 2d 408, 2006 WL 544551 (Fla. Dist. Ct. App. 2006) (citing Curry v. State, 811 So. 2d 736, 741 (Fla. Dist. Ct. App. 2002)).
[117] 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 ____, at 380; Tucker, *supra* note ____, at 653. It is beyond the scope of this paper to consider what the penalties should be to address and deter cyberstalking crimes.
[118] *See* FLA. STAT. ANN. § 784.048 (West 2005); 720 ILL. COMP. STAT. ANN. 5/12-7.5 (West 2005); NEV. REV. STAT. ANN. § 200.575(3) (West 2005); OHIO REV. CODE ANN. § 2903.211 (West 2005); R.I. GEN. LAWS § 11-52-4.2 (2004); VA. CODE ANN. § 18.2-152.7:1 (West 2005); *see also infra* Appendix to this article. *But cf.* COLO. REV. STAT. ANN. § 18-13-105 (West 2005) (not a stalking statute, but may apply to third party harassment).
[119] 720 ILL. COMP. STAT. ANN. 5/12-7.5(b) (West 2005). The Illinois statute does criminalize a course of conduct which "alarms, torments, or terrorizes that person." 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.
[120] LA. REV. STAT. ANN. § 14:40.3(b)(2)-(3) (2005); N.C. GEN. STAT. ANN. § 14-196.3(b)(2)-(3) (West 2005).

cyberstalking statute also seems to suggest that the stalker has to specifically e-mail the victim.[121] The Florida statute has similar problems since it requires that electronic communications be "directed at a specific person."[122] 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.[123]

At the end of the day, only three states (Ohio,[124] Rhode Island,[125] and Washington[126]) 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.[127]

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 on the victim's fear, rather than a subjective standard which focuses on the perpetrator's actions. Thus, cyberstalking

---

[121] MISS. CODE ANN. § 97-45-15 (West 2005).
[122] FLA. STAT. ANN. § 784.048(1)(d) (West 2005).
[123] HITCHCOCK, *supra* note ____, at 112.
[124] OHIO REV. CODE ANN. § 2903.211(A)(2) (West 2005) ("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. § 2903.211(A)(2)(b).
[125] R.I. GEN. LAWS § 11-52-4.2(a) (2004) ("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).
[126] WASH. REV. CODE ANN. § 9.61.260(1)(a) (West 2005) ("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).
[127] 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. ANN. 135/1-2(3.1) (West 2005); VT. STAT. ANN. tit. 13, § 1027(a)(iii) (2005); WASH. REV. CODE ANN. § 9.61.260(1)(b) (West 2005).

statutes should adopt a reasonable person standard.[128] Another way to address the gaps in the state statutes is to enact laws that specifically criminalize conduct where perpetrators ruse "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.[129] 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.[130] 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.

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 prosecuting cyberstalkers. This next section takes each of the three federal statutes,

---

[128] Some cyberstalking statutes have adopted a related standard that is just as effective. A few statutes criminalize conduct that causes the victim to suffer substantial or severe emotional distress. *See*, *e.g.,* N.C. GEN. STAT. ANN. § 14-277.3 (West 2005). This standard will work in cyberstalking cases because, like the reasonable person standard, the focus is on the fear instilled in the victim, rather than the cyberstalker's conduct.

[129] "[C]yberstalking does not end in cyberspace, but usually transcends into real life." Lee, *supra* note ____, at 407.

[130] *See* Walsh, *supra* note ____, at 386-87 ("In many cases, this ambiguity [in offline stalking laws] actually allowed offenders to 'slip through the cracks' of justice, by permitting the judicial system to vindicate only the rights of those stalking victims who fell prey to behavior criminalized in that particular state. Persons who engaged in behavior that would be characterized as stalking suffered no legal consequences when that behavior was not statutorily criminalized.").

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 containing "any threat" to injure another person.[131] "Any communication" includes threats transmitted across state lines via the telephone, e-mail, beepers, or the Internet.[132] This statute successfully prosecuted at least one cyberstalker who used the Internet to send threatening e-mail messages.[133]

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.

United States v. Alkhabaz[134] 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. 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.[135] Despite the sadistic story

[131] 18 U.S.C. § 875(c) (2006).
[132] *Id.*
[133] *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).
[134] United States v. Alkhabaz, 104 F.3d 1492 (6th Cir. 1997).
[135] *Id.* at 1498 (Krupansky, J., dissenting).

about the defendant's classmate, the court held that he was not in violation of § 875(c), because he did not make a "communication containing a true threat."[136]

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.

2. Gaps in the Federal Telephone Harassment Statute, 47 U.S.C. § 223.

The Telephone Harassment Statute[137] 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, harass, or threaten" a person.[138]

Very recently, 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 Women Act" a section entitled, "Preventing Cyberstalking,"[139] amended the statute[140] to apply to e-mail messages.[141] Specifically, the definition of the "telecommunications device" was changed to include "any device or software that can be used to originate

---

[136] *Id.* at 1497.
[137] 47 U.S.C. § 223 (2006).
[138] 47 U.S.C. § 223(a)(1)(C).
[139] Violence Against Women and Department of Justice Reauthorization Act of 2005, Pub. L. No. 109-162, Title I, § 113, 119 Stat. 2987 (2006) [hereinafter *Violence Against Women Act*]. As the Summary of the act explains, "(Sec. 113) Amends the Communications Act of 1934 to apply the prohibitions against certain communications in interstate of foreign commerce to communications transmitted by the Internet (i.e., cyberstalking)." *Id.* at 2.
[140] The House approved it by voice vote, and the Senate unanimously approved it on December 16, 2005. *See* Declan McCullagh, *Create an E-annoyance, Go to Jail*, http:news.com.com/Create+an+e-annoyance%2C+go+jail/2010-1028_3-6022491.html.
[141] *Violence Against Women Act*, *supra* note ____.

telecommunications or other types of communications that are transmitted, in whole or in part, by the Internet."[142]

While the amendment changed the definition of a "telecommunications device" to specifically include e-mail,[143] 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, harass or threaten" a person.[144] The amendment has created some controversy. Proponents call it an answer to many victims' cries for "help."[145] 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."[146]

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,[147] the Sixth Circuit found that the word "annoy" in the statute was not unconstitutional because: (1) it upheld Congressional intent to "protect innocent individuals from fear" without being vague or overbroad; and (2) it did not chill political

---

[142] *Id.* (adding this language to 47 U.S.C. § 223h(3)(C)).

[143] Even without this amendment, the courts may have interpreted the Internet as a "telecommunication device." *See* Am. Civil Liberties Union 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.") (citing 141 Cong.Rec. S8329-46 (daily ed. June 14, 1995) (statements of Sen. Exon and Sen. Coats)).

[144] 47 U.S.C. § 223a(1)(C).

[145] Dalton Jr., *supra* note ____ (citing a spokesman from the offices of the Washington Congressman Rep. Jim McDermott who joined in sponsoring the amendment to the Telephone Harassment Statute).

[146] Tom Zeller, Jr., *A Sinister Web Entraps Victims of Cyberstalkers*, N.Y. TIMES, Apr. 17, 2006. *See also* Dalton Jr., *supra* note ____ (explaining that a Website, TheAnonymousE-mail.com, which allows users to send anonymous messages, has filed a challenge to the amendment); K.C. Jones, *Cyberstalking Law Targets E-Mail, but Could Chill Bloggers*, http://www.informationweek.com/story/showArticle.jhtml?articleID=177103642; McCullagh, *supra* note ____ (quoting an ACLU representative, "The use of the word 'annoy' is particularly problematic . . . What's annoying to one person may not be annoying to someone else.").

[147] United States v. Bowker, 372 F.3d 365 (6th Cir. 2004) *remanded on other grounds in* United States v. Bowker, 125 Fed. Appx. 701 (6th Cir. 2005) (upholding criminal convictions, but remanded to district court for re-sentencing). *See also* United States v. Lampley, 573 F.2d 783 (3rd Cir. 1978) (upholding constitutionality of the statute).

or free speech.[148] 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*.[149] It seems odd to only make cyberstalking a crime where the identity of the cyberstalker is unknown.[150] 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.[151] Thus, the amended statute is inadequate to deal with behavior where the cyberstalker indirectly harasses or terrorizes his victim by posting messages on

---

[148] The court explained that the word "annoy" standing alone might pose vagueness concerns. 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." *Bowker*, 372 F.3d. at 382-83 (internal citations 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.* 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.

[149] 42 U.S.C. § 223(a)(1)(C) (2006). *See also* Jones, *supra* note ____ (citing Jeff Lundgren, communications director for the U.S. House Judiciary Committee, who states that the amendment "doesn't target any Internet except e-mail").

[150] However, one court has held that the lack of the anonymity element made a state statute unconstitutional under the New Hampshire State Constitution. *See* New Hampshire v. Brobst, 857 A.2d 1253 (N.H. 2004) (note, this case did not deal with the constitutionality of the statute under the U.S. Constitution).

[151] 42 U.S.C. § 223(a)(1)(C) (2006).

a bulletin board, creating a Website 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.[152] 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.[153] 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.

3. Gaps in the Federal Interstate Stalking Punishment and Prevention Act, 18 U.S.C. § 2261A.

The most promising federal statute to combat cyberstalking, is the "Interstate Stalking Punishment and Prevention Act."[154] 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."[155] 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. The statute was formerly only triggered when a stalker

---

[152] 42 U.S.C.A. § 223(a) (2006).
[153] *See* The Interstate Stalking Punishment and Prevention Act, 18 U.S.C.A. § 2261A (2006); 18 U.S.C.A. § 2261(b) (2006) (setting forth the penalties for violating § 2261A).
[154] 18 U.S.C. § 2261A (2006).
[155] 18 U.S.C. § 2261A(1), (2)(A)-(B) (1996).

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."[156] 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; [157] however, in that case, the defendant had traveled across state lines.[158]

The second amendment to § 2261A occurred recently in January 2006. [159] 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 harm." [160] 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.

---

[156] Victims of Trafficking and Violence Protection Act of 2000, Pub. L. No. 106-386, Div. B, Title I, § 1107(b)(1), 114 Stat. 1498 (2000).
[157] 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)." *United States v. Bowker*, 372 F.3d 365, 377, n.2 (6th Cir. 2004) (distinguished on other grounds).
[158] *Id.* at 374.
[159] *Violence Against Women Act*, *supra* note ____.
[160] *Id.*

Thus, the newly amended § 2261A address many of the shortcomings of the other federal statutes. It does not have a "true/credible threat" requirement;[161] but rather adopts a standard that measures the victim's "reasonable fear" or "substantial emotional harm."[162] Nor does it limit coverage of the "use" of the computer to only anonymous e-mail messages.[163]

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

[161] 18 U.S.C. § 875(c) (2006).
[162] 18 U.S.C. § 2261A(1), (2)(A)-(B) (2006).
[163] *Compare* 18 U.S.C. § 2261(B) *with* 42 U.S.C. § 223(a)(1)(C) (2006).

protective orders.[164] 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 call for information that is difficult or impossible to obtain due to the anonymous nature of a cyberstalker.[165]

In Virginia, for example, the law provides that a Stalking Protective Order may be issued after a criminal conviction for stalking.[166] Alternatively, the victim would have to prove, by a preponderance of the evidence, that the perpetrator is guilty of stalking.[167] 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.[168] In fact, is unclear if Virginia's stalking statute specifically covers electronic communications.[169] Thus, cyberstalking victims may have to wait until the cyberstalker is formally prosecuted before they can secure any sort of protective order.[170]

---

[164] *See generally* Lowell T. Woods, Note, *Anti-Stalker Legislation: A Legislative Attempt to Surmount the Inadequacies of Protective Orders*, 27 IND. L.J. 449 (1993).

[165] 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 Ann. § 34-26-5 (West 2006), http://www.in.gov/judiciary/forms/po/po/po-0102.doc 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.

[166] *See Domestic Violence and Family Abuse,* http://www.courts.state.va.us/courts/jdr/Lynchburg/violence.html#ppo.

[167] *Id.*

[168] VA. CODE ANN. § 18.2-60.3 (West 2005).

[169] *Id. See infra* Appendix to this Article.

[170] 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 Domestic Violence Unit,* http://www.lvmpd.com/Bureaus_and_Staff/Domestic_Violence/Protective_Orders.html. Likewise in Texas, to 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. The protective order is defined in terms of family violence, and makes no mention of resources for cyberstalking. *See Attorney General of Texas*, http://www.oag.state.tx.us/victims/protective.shtml#law. 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. *See Protective Orders,* http://www.courts.state.md.us/courtforms/joint/ccdcdv01br.pdf.

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.[171] 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 related to protective orders in cyberstalking cases at all.[172] Thus, a cyberstalking victim may not be able to obtain a proactive order via current federal laws.

Another potential issue concerns *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.[173] Potentially this means that if the perpetrator uses a cable connection (as opposed to a dial-up connection via the telephone lines) to access the Internet, law enforcement agents have to notify the potential cyberstalker before being able to access computer records (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.[174]

---

[171] H.R. 3747, 105th Cong (1998); H.R. 1869, 106th Cong. (1999).
[172] *See* Victims of Trafficking and Violence Protection Act of 2000, Pub. L. No. 106-386, Div. B, Title I, § 1107(b)(1), 114 Stat. 1498 (2000).
[173] Cable Communications Policy Act of 1984, 47 U.S.C. § 551(h) (2006).
[174] *See, e.g.,* Patriot Act of 2001, Pub. L. No. 107-56 (2001); *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 (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. *See In re Application*, 158 F. Supp. 2d at 648; 18 U.S.C. § 2705(b). 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

IV. Problems with Criminalizing Cyberstalking

There are at least two potential concerns related 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.[175]

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.[176] 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.[177]

---

court order. *See* Patriot Act of 2001, Pub. L. No. 107-56 § 211; *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.

[175] *See, e.g.,* Am. Civil Liberties Union v. Reno*,* 521 U.S. 844 (1997) (holding that the Internet is an important tool for protected speech activities); Watts v. United States, 394 U.S. 705 (1969).
[176] Lisa A. Karczewski, *Stalking in Cyberspace: The Expansion of California's Current Anti-Stalking Laws in the Age of the Internet*, 30 MCGEORGE L. REV. 517 (1999).
[177] Karczewski, *supra* note ____, at 517.

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) an provision stating that the law does not include "constitutionally protected activity", including, but not limited to "picketing and organized protests."[178] Moreover, many current offline stalking statutes contain specific language that the statute cannot violate constitutional rights. [179] This may be another element that should be included in newly enacted cyberstalking statutes.

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.[180] 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.[181] However, there are some reports that suggest that cyberstalking is ever growing. The CyberAngels, a non-

[178] Tucker, *supra* note ____, at 622, 630-31.
[179] GA. CODE ANN. § 16-5-92 (West 2005); IDAHO CODE ANN. § 18-7906(2)(a) (2005); IND. CODE ANN. § 35-45-10-1 (West 2005); KY. REV. STAT. ANN. § 508.130(1)(b)(2) (West 2005); ME. REV. STAT. ANN. tit. 17-A, § 210-A(2)(A) (2005); MISS. CODE ANN. § 97-3-107 (West 2005); MO. ANN. STAT. § 565.225 (West 2005); MONT. CODE ANN. § 45-5-220 (2005); NEB. REV. STAT. ANN. § 28-311.02(1) (2005); NEV. REV. STAT. ANN. § 200.575(6)(e) (West 2005); N.H. REV. STAT. ANN. § 633:3-a(II)(a) (2005); N.M. STAT. ANN. § 30-3A-4 (West 2005); N.D. CENT. CODE § 12.1-17-07.1(1)(a), (5) (2005); OR. REV. STAT. ANN. § 163.755 (West 2003); R.I. GEN. LAWS § 11-52-4.2 (2004) (cyberstalking statute); S.D. CODIFIED LAWS § 22-19A-5 (2005); W. VA. CODE ANN. § 61-2-9a(h) (LexisNexis 2005).
[180] *1999 Report on Cyberstalking*, *supra* note ____, at 12.
[181] *Id.*.

profit organization that assists cyberstalking victims,[182] estimates that there are approximately 63,000 Internet stalkers in the United States and 474,000 victims world-wide.[183]

V. CONCLUSION

As technology changes, so do 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.

APPENDIX (starts on next page)

[182] The CyberAngels Website is at www.cyberangels.org.
[183] Tjaden & Thoennes, *supra* note ____, at 2.

	Alabama	Alabama	Alaska	Alaska	Arizona
Code	ALA. CODE § 13A-11-8(b)(1) (2005).	ALA. CODE § 13A-6-90 (2005).	ALASKA STAT. §§ 11.41.260 to 41.270 (2004).	ALASKA STAT. § 11.61.120(a)(4) (2004).	ARIZ. REV. STAT. ANN. § 13-2921 (2005).
Title	Harassing Communications (misdemeanor)	Stalking (felony)	1st Degree Stalking 2nd Degree Stalking	Harassment	Harassment
Reasonable Person Standard?	Yes, but requires a "threat"	Yes, but requires a "credible threat." *See* ALA. CODE § 13A-6-92(b) (2005).	No	No	Yes "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."
Credible Threat Standard?	Requires a "threat"	Yes	No	Yes, requires a "threat" of physical injury or sexual contact	No
Requires Actual Physical Pursuit?	No	No	No	No	No
Statute Covers Electronic Communications?	Yes "Communicates with a person, anonymously or otherwise, by telephone, mail, or any other form of written or electronic communication"	No	Yes, but only covers "electronic communications" to victim. See ALASKA STAT. §§ 11.41.260 to 41.270(3)(f) (2004).	Yes, but only to "electronic communications" to victim	Yes
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.

Code	Arizona ARIZ. REV. STAT. ANN. § 13-2923 (2005).	Arkansas ARK. CODE ANN. § 5-71-229 (West 2005).	Arkansas ARK. CODE ANN. § 5-71-209(a)(1) (West 2005).	Arkansas ARK. CODE ANN. § 5-41-108(a)(1)(A)-(D) (West 2005).	California CAL. PENAL CODE § 646.9 (West 2005).
Title	Stalking	Stalking (felony)	Harassing Communications (misdemeanor)	Unlawful Computerized Communications (misdemeanor)	Stalking
Reasonable Person Standard?	Yes, but only when the conduct includes repeatedly maintaining a visual or physical proximity to a person, otherwise a threat is required.	No	No	No	Yes, but also requires a credible threat
Credible Threat Standard?	Sometimes Conduct includes repeatedly maintaining a visual or physical proximity to a person conveying verbal or written threats or threats implied by conduct.	Yes "Terrorist threat"	No, requires intent to annoy	Sometimes "Message threatens to cause injury to any person or damage to any property of any person or uses obscene, lewd, or profane language"	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 to reasonably fear for her safety or her family's safety"
Requires Actual Physical Pursuit?	No	No	No	No	No
Statute Covers Electronic Communications?	Not specifically, but does cover "written threats."	Not specifically	Not specifically, but does apply to any "form of written communication" to the victim.	Yes, but only applies to "computerized communications" sent to the victim	Yes Includes computers defined by 18 U.S.C. § 2510(12) (2006).
Notes	Requires an actual threat when the perpetrator is not physical pursuit.				
Potential Statutory Problems	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.	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 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.	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.	1. Requires a credible threat. 2. May not apply when a cyberstalker dupes an "innocent" third party to harass.

	California	Colorado	Colorado	Connecticut	Connecticut
Code	CAL. PENAL CODE § 653m (West 2005).	COLO. REV. STAT. ANN. § 18-9-111(1)(e) (West 2005).	COLO. REV. STAT. ANN. § 18-13-105 (West 2005).	CONN. GEN. STAT. ANN. § 53a-181c (West 2005).	CONN. GEN. STAT. ANN. § 53a-181d (West 2005).
Title	Telephone Calls or Contact by Electronic Communication Device with Intent to Annoy (misdemeanor)	Harassment — Stalking	Criminal Libel (felony)	1st Deg. Stalking (felony)	2nd Deg. Stalking (misdemeanor)
Reasonable Person Standard?	No	Yes (Stalking) No (Harassment)	No	Yes	Yes
Credible Threat Standard?	No, requires intent to annoy	Yes (Stalking) No (Harassment)	No	No	No
Requires Actual Physical Pursuit?	No	No	No	Yes "follows or lies in wait"	Yes "follows or lies in wait"
Statute Covers Electronic Communications?	Yes, but only applies to "contact" with the victim	Possibly (Stalking) Yes (Harassment) Computer, computer network, or computer system	Not specifically, but applies to "written instrument"	No	No
Notes		The statute specifically notes seriousness of stalking. *See* § 18-9-111(4)(a).	Standard: "A person who shall knowingly publish or disseminate, either by written instrument, sign, pictures, or the like, any statement or object tending…to impeach the honesty, integrity, virtue, or reputation. . .of one who is alive, and thereby to expose him to public hatred, contempt, or ridicule, commits criminal libel."		
Potential Statutory Problems	1 Reasonable standard would be more applicable. 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.	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.	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.	1. Electronic communications are not 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.

	Connecticut	Connecticut	Connecticut	Delaware	Delaware
Code	CONN. GEN. STAT. ANN. § 53a-181e (West 2005).	CONN. GEN. STAT. ANN. § 53a-182b (West 2005).	CONN. GEN. STAT. ANN. § 53a-183 (West 2005).	DEL. CODE ANN. tit. 11, § 1312A (2005).	DEL. CODE ANN. tit. 11, §§ 1311-12 (2005).
Title	3rd Deg. Stalking (misdemeanor)	1st Deg. Harassment (felony)	2nd Deg. Harassment (misdemeanor)	Stalking (felony or misdemeanor)	Harassment (misdemeanor)
Reasonable Person Standard?	Yes	No	No	Sometimes Only when the conduct includes repeatedly maintaining a visual or physical proximity to a person, otherwise a threat is required	Yes 2004 amendment added the phrase, "or cause a reasonable person to suffer substantial emotional distress"
Credible Threat Standard?	No	Yes "he threatens to kill or physically injure"	No	Sometimes Either physical proximity or threat	No
Requires Actual Physical Pursuit?	Yes "follows or lies in wait"	No	No	Sometimes Either proximity or a threat	No
Statute Covers Electronic Communications?	No	Yes Covers "computer network"	Yes	No	Yes Communicate with a person by electronic communication in a manner which the person knows is likely to cause annoyance or alarm
Notes			Broad statute covering communications made "in a manner likely to cause 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.
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. Requires direct contact with the victim. 2. May not apply when a cyberstalker dupes an "innocent" third party to harass.	1. 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.	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.

	District of Columbia	Florida	Florida	Georgia	Georgia
Code	D.C. CODE § 22-404 (2005).	FLA. STAT. ANN. § 784.048 (West 2005).	FLA. STAT. ANN. § 836.10 (West 2005).	GA. CODE ANN. § 16-5-90 (West 2005).	GA. CODE ANN. § 16-5-91 (West 2005).
Title	Assault or Threatened Assault in a Menacing Manner — Stalking	Stalking	Harassment	Stalking (misdemeanor)	Aggravated Stalking (felony)
Reasonable Person Standard?	Yes	Yes But, for a felony charge requires a credible threat.	No	Yes Conduct that "harass[es] or intimidat[es]." § 16-5-90(a).	No
Credible Threat Standard?	No	No - misdemeanor stalking Yes - felony stalking	Yes	No	No
Requires Actual Physical Pursuit?	No	No	No	No	No
Statute Covers Electronic Communic-ations?	Unclear, does not specify how the communication must be made	Yes	Not specifically, but does cover "inscribed communication"	Yes	Yes
Notes		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."		Computer and computer network defined by GA. CODE ANN. § 16-9-92 (West 2005) (added 2000); contact occurs at the place or places where the communication is received	
Potential Statutory Problems	1. Unclear if electronic communications are covered. 2. May not apply when a cyberstalker dupes an "innocent" third party to harass.	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. 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.

	Hawaii	Hawaii	Idaho	Illinois	Illinois
Code	HAW. REV. STAT. ANN. §§ 711-1106.4 to -1106.5 (LexisNexis 2005).	HAW. REV. STAT. ANN. § 711-1106 (LexisNexis 2005).	IDAHO CODE ANN. §§ 18-7905 to -7906 (2005).	720 ILL. COMP. STAT. ANN. 5/12-7.5 (West 2005).	720 ILL. COMP. STAT. ANN. 135/1-2 (West 2005).
Title	Harassment by Stalking Aggravated Harassment by Stalking	Harassment	1st Deg. Stalking 2nd Deg. Stalking	Cyberstalking (felony)	Harassment Through Electronic Communications
Reasonable Person Standard?	No	Yes	Yes	Yes (either reasonable person or credible threat)	No, but has broad standard that covers the intent "to harass"
Credible Threat Standard?	No	Not specifically, but see "Notes"	No	Yes (either reasonable person or credible threat)	Yes (either intent to harass or direct threat)
Requires Actual Physical Pursuit?	Sometimes Either pursuit, or non-consensual contact —	No	No	No	No
Statute Covers Electronic Communications?	Yes Non-consensual contact includes contact via e-mail transmission; amended in 2003	Yes Repeatedly makes e-mail transmissions without legitimate purpose	Yes Nonconsensual conduct includes but is not limited to sending electronic communications	Yes	Yes Same as 720 ILL. COMP. STAT. ANN. 5/12-7.5 (West 2005).
Notes	Aggravated harassment by stalking requires a current and prior conviction for the offense of harassment by stalking	Must prove the victim reasonably believed that defendant intended to cause bodily injury. *See State v. Bush*, 50 P.3d 428 (Haw. Ct. App. 2002).	Course of conduct involved "nonconsensual contact." IDAHO CODE ANN. § 18-7906(2)(a) (2005).	May apply when a cyberstalker dupes an "innocent" third party to harass since statute is broadly written to include a "course of conduct" "that alarms, torments, or terrorizes that person." § 5/12-7.5(b).	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.
Potential Statutory Problems	1. May not apply when a cyberstalker dupes an "innocent" third party to harass.	1. May require threat. 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. 2. May only apply to direct contact with the victim (e-mail), not other Internet postings.	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).

	Indiana	Indiana	Iowa	Iowa	Kansas
Code	IND. CODE ANN. § 35-45-10-1, -5 (West 2005).	IND. CODE ANN. § 35-45-2-2 (West 2005).	IOWA CODE ANN. § 708.7 (West 2005).	IOWA CODE ANN. § 708.11 (West 2005).	KAN. STAT. ANN. § 21-3438 (West 2005).
Title	Stalking (felony)	Harassment (misdemeanor)	Harassment	Stalking	Stalking
Reasonable Person Standard?	Yes	No, but has broad standard that covers the intent "to harass"	No, but has broad standard that covers the intent "to harass"	Yes, but requires a threat. *See* § 708.11(1)(b), 2(a).	No
Credible Threat Standard?	Yes, for a felony. *See* IND. CODE ANN. § 35-45-10-5(b)(1)(B).	No	Yes, for first and second degree harassment No, for third degree harassment	Yes, either visual proximity or threat	Yes
Requires Actual Physical Pursuit?	No	No	No	Yes, either visual proximity or threat	No
Statute Covers Electronic Communications?	Yes	Yes Computer network is defined in IND. CODE ANN. § 35-43-2-3(a) (West 2005).	Yes	Not specifically	Yes Electronic communication includes, but is not limited to, computers and computer networks
Notes			Sometimes requires personal contact — an encounter where two or more people are in visual or physical proximity to each other; personal contact does not require a physical touching or communication		
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. May not apply when a cyberstalker dupes an "innocent" third party to harass. 2. May only apply to direct communication with the victim (e-mail), not other Internet postings. § 708.7 1(a)(1).	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. Requires a threat. 2. May not apply when a cyberstalker dupes an "innocent" third party to harass.

	Kentucky	Kentucky	Louisiana	Louisiana	Maine	Maryland
Code	KY. REV. STAT. ANN. §§ 508.130-.150 (West 2005).	KY. REV. STAT. ANN. §§ 525.080 (West 2005).	LA. REV. STAT. ANN. § 14:40.2 (2005).	LA. REV. STAT. ANN. § 14:40.3 (2005).	ME. REV. STAT. ANN. tit. 17-A, §§ 210-210-A (2005).	MD. CODE ANN., CRIM. LAW § 3-805 (West 2005).
Title	1st Deg. Stalking 2nd Deg. Stalking	Harassing Communications (misdemeanor)	Stalking	Cyberstalking	Terrorizing (§ 210) Stalking (§ 210A)	Misuse of Electronic Mail
Reasonable Person Standard?	Yes, but also requires an explicit threat	No, but has broad standard that covers the intent "to harass"	Yes	No, but has broad standard that covers the intent "to harass"	Yes, but requires threat.	No
Credible Threat Standard?	Yes	No	No	No	Yes Conduct requires either visual proximity or a threat	No
Requires Actual Physical Pursuit?	No	No	No	No	No	No
Statute Covers Electronic Communications?	No	Yes	Unclear	Yes	Yes	Yes E-mail means transmission by computer or other electronic means received by a person with a unique address
Notes				Similar to North Carolina's cyberstalking statute		
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.	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.

	Maryland	Maryland	Massachusetts	Massachusetts	Michigan
Code	MD. CODE ANN., CRIM. LAW § 3-802 (West 2005)	MD. CODE ANN., CRIM. LAW § 3-803 (West 2005).	MASS. GEN. LAWS ANN. ch. 265, § 43 (West 2005).	MASS. GEN. LAWS ANN. ch. 265, § 43A (West 2005).	MICH. COMP. LAWS ANN. § 750.411h-i (West 2005).
Title	Stalking	Harassment (misdemeanor)	Stalking	Criminal Harassment	Stalking (misdemeanor) Aggravated Stalking (felony)
Reasonable Person Standard?	Yes	No, but has broad standard that covers the intent "to harass"	Yes, but requires a threat	Yes	Yes (Stalking) No (Aggravated Stalking)
Credible Threat Standard?	No	No	Yes	No	No (Stalking) Yes (Aggravated Stalking)
Requires Actual Physical Pursuit?	Yes Approaching or pursuing another	No	No	No	No
Statute Covers Electronic Communications?	No	Unclear	Yes	Yes	Yes Non-consensual conduct includes sending mail or electronic communications
Notes		Requires that stalker be warned/asked to stop conduct			
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.	1. Requires a 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. May only apply to direct "contact" with the victim (e-mail), not other Internet postings. § 750.411h(1)(c). 2. May not apply when a cyberstalker dupes an "innocent" third party to harass.

	Minnesota	Mississippi	Mississippi	Mississippi	Missouri	Montana
Code	MINN. STAT. ANN. § 609.749 (West 2005).	MISS. CODE ANN. § 97-3-107 (West 2005).	MISS. CODE ANN. §§ 97-3-85, 97-29-45 (West 2005).	MISS. CODE ANN. § 97-45-15 (West 2005).	MO. ANN. STAT. § 565.225 (West 2005).	MONT. CODE ANN. § 45-5-220 (2005).
Title	Harassment — Stalking	Stalking	Threats; obscene communications	Cyberstalking (felony)	Stalking	Stalking
Reasonable Person Standard?	Yes Actor knows or has reason to know it would cause victim under the circumstances to feel fear, and actually causes fear	Sometimes (see "credible threat")	No, but has broad standard that covers the intent "to terrorize" or "to harass"	No, but has broad standard that covers the intent "to harass"	Yes, for stalking Yes, plus credible threat for aggravated stalking	Yes
Credible Threat Standard?	No	Sometimes 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	No	Sometimes Requires language threatening to inflict injury or for extortion; to knowingly make false statements intending to threaten, terrify, or harass; larger penalty if there is a credible threat	Yes, for aggravated stalking	No
Requires Actual Physical Pursuit?	No	No	No	No	No	No
Statute Covers Electronic Communic-ations?	Yes	Unclear	Yes	Yes Electronic communication has to be received by a person with a unique address	Yes	Yes
Potential Statutory Problems	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. Electronic communications are not explicitly covered. 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 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.	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.

	Montana	Nebraska	Nevada	Nevada	New Hampshire
Code	MONT. CODE ANN. § 45-8-213 (2005).	NEB. REV. STAT. ANN. §§ 28-311.02-03 (2005).	NEV. REV. STAT. ANN. § 200.575 (West 2005).	NEV. REV. STAT. ANN. § 200.571 (West 2005).	N.H. REV. STAT. ANN. § 633:3-a (2005).
Title	Privacy in Communications	Stalking	Stalking	Harassment	Stalking
Reasonable Person Standard?	No	No, but has broad standard that covers conduct that "seriously terrifies, threatens, or intimidates." § 28-311.02(2)(a).	Yes (Stalking, misdemeanor) No (Aggravated Stalking, felony)	No	Yes
Credible Threat Standard?	Sometimes use of obscene or lewd language or a threat	No	No (Stalking) Yes (Aggravated Stalking)	Yes	No
Requires Actual Physical Pursuit?	No	No	No	No	No
Statute Covers Electronic Communic-ations?	Yes	Unclear	Yes "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)	No	Yes
Notes			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 other Internet postings. 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.	Although "cyberstalking" is not specifically mentioned, this statute may apply to most aspects of cyberstalking.	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 when a cyberstalker dupes an "innocent" third party to harass. [Note, N.H. harassment statute held unconstitutional. *State v. Pierce*, 887 A.2d 132 (N.H. 2005) (finding N.H. REV. STAT. ANN. § 644:4 (2005), unconstitutional).

	New Jersey	New Jersey	New Mexico	New Mexico	New York	New York
Code	N.J. STAT. ANN. § 2C:12-10 (West 2005).	N.J. STAT. ANN. § 2C:33-4 (West 2005).	N.M. STAT. ANN. §§ 30-3A-3 (West 2005).	N.M. STAT. ANN. § 30-3A-2 (West 2005).	N.Y. PENAL LAW §§ 240.25-26 (McKinney 2005).	N.Y. PENAL LAW § 240.30 (McKinney 2005).
Title	Stalking	Harassment (misdemeanor)	Stalking	Harassment (misdemeanor)	Harassment	Aggravated Harassment
Reasonable Person Standard?	No	No, but has broad standard that covers conduct that "causes annoyance"	Yes	Yes	Yes	No, but has broad standard that covers conduct with the intent "to harass"
Credible Threat Standard?	Yes	No	No	No	No	No
Requires Actual Physical Pursuit?	Sometimes Either maintain physical proximity or threaten	No	No	No	No	No
Statute Covers Electronic Communications?	Not specifically	Not specifically	Not specifically	Not specifically	Not specifically	Yes
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.	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 to electronic communications. 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.

	New York	New York	New York	North Carolina	North Carolina
Code	N.Y. PENAL LAW §§ 120.45-50 (McKinney 2005).	N.Y. PENAL LAW § 120.55 (McKinney 2005).	N.Y. PENAL LAW § 120.60 (McKinney 2005).	N.C. GEN. STAT. ANN. § 14-277.3 (West 2005).	N.C. GEN. STAT. ANN. § 14-196.3 (West 2005).
Title	4th & 3rd Deg. Stalking (misdemeanors)	2rd Deg. Stalking (felony)	1st Deg. Stalking (felony)	Stalking	Cyberstalking
Reasonable Person Standard?	Yes	Yes	Yes	Yes	No, but has broad standard that covers the intent "to harass"
Credible Threat Standard?	No	No	No	No	No
Requires Actual Physical Pursuit?	No	Yes, must display a weapon	Yes, must cause physical injury	Sometimes Either harasses or physically follows	No
Statute Covers Electronic Communications?	Likely	No	No	Yes	Yes
Notes					Similar to Louisiana's cyberstalking statute
Potential Statutory Problems	1. May not apply when a cyberstalker dupes an "innocent" third party to harass.	1. Requires physical display of weapon. 2. May not apply to electronic communications. 3. May not apply when a cyberstalker dupes an "innocent" third party to harass.	1. Requires physical display of weapon. 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 when a cyberstalker dupes an "innocent" third party to harass.	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.

	North Dakota	North Dakota	Ohio	Ohio	Oklahoma	Oklahoma
Code	N.D. CENT. CODE § 12.1-17-07.1 (2005).	N.D. CENT. CODE § 12.1-17-07 (2005).	OHIO REV. CODE ANN. § 2903.211 (West 2005).	OHIO REV. CODE ANN. § 2917.21 (West 2005).	OKLA. STAT. ANN. tit. 21, §§ 1172-73 (West 2005).	OKLA. STAT. ANN. tit. 21, § 1953(8)-(9) (West 2005).
Title	Stalking	Harassment	Menacing by Stalking	Telecommunications Harassment	Harassment Stalking	Computer Crimes Act (misdemeanor)
Reasonable Person Standard?	Yes	No, uses broad standard that covers the intent "to harass," but requires a threat	Similar standard (conduct that would "cause another person to believe that the offender will cause physical harm"). § 2903.211(A)(1).	No, but uses broad standard that covers the intent "to harass"	Yes	No, but uses broad standard that covers the intent "to harass"
Credible Threat Standard?	No	Yes	Yes, for 4th Deg. Stalking (felony), a threat is required. § 2903.211(A)(2)(b).	No	No	No
Requires Actual Physical Pursuit?	No	No	No	No	No	No
Statute Covers Electronic Communic-ations?	Not specifically	Yes	Yes	Yes *See* OHIO REV. CODE ANN. § 2913.01 (West 2005).	Yes	Yes
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. 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.	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. § 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).	1. 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.	1. May not apply when a cyberstalker dupes an "innocent" third party to harass.

	Oregon	Oregon	Pennsylvania	Rhode Island	Rhode Island	South Carolina
Code	OR. REV. STAT. ANN. § 163.732 (West 2003).	OR. REV. STAT. ANN. § 166.065(1)(c) (West 2003).	18 PA. CONS. STAT. ANN. §§ 2709 to 2709.1 (West 2005).	R.I. GEN. LAWS §§ 11-59-1 and 2 (2004).	R.I. GEN. LAWS § 11-52-4.2 (2004).	S.C. CODE ANN. § 16-3-1700 (2005).
Title	Stalking	Harassment	Stalking Harassing	Stalking	Cyberstalking	Harassment Stalking
Reasonable Person Standard?	Yes, but requires direct contact	No	Yes	No, but has broad harassment standard	Yes	Yes
Credible Threat Standard?	Yes 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).	Yes	No	No	No	No
Requires Actual Physical Pursuit?	No	No	No	Yes, physical following when reasonable person standard is used. § 11-59-2(a)(2).	No	No
Statute Covers Electronic Communic-ations?	Yes. *See* OR. REV. STAT. ANN. § 163.730 (West 2003).	Yes	Yes	Not specifically	Yes	Yes, for 2nd Deg. Harassment (misdemeanor)
Potential Statutory Problems	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.	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).	1. May not apply when a cyberstalker dupes an "innocent" third party to harass

	South Dakota	Tennessee	Tennessee	Texas	Texas	Utah
Code	S.D. CODIFIED LAWS § 22-19A-1 (2005).	TENN. CODE ANN. § 39-17-315 (West 2005).	TENN. CODE ANN. § 39-17-308 (West 2005).	TEX. PENAL CODE ANN. § 42.072 (Vernon 2005).	TEX. PENAL CODE ANN. § 42.07 (Vernon 2005).	UTAH CODE ANN. § 76-5-106 (West 2005).
Title	Stalking	Stalking	Harassment	Stalking	Harassment	Harassment
Reasonable Person Standard?	Yes, but requires threat; also has broad harassment standard	Yes, but requires contact	No	Yes	No	No
Credible Threat Standard?	Yes (one option; see "reasonable person standard")	No (Stalking) Yes (Aggravated Stalking)	Yes	No	Yes	Yes
Requires Actual Physical Pursuit?	No	No	No	No	No	No
Statute Covers Electronic Communications?	Yes	Yes Non-consensual contact includes sending electronic communications	Yes	Not specifically	Yes Electronic communication includes a communication initiated by e-mail or instant message	Not specifically
Notes					Statute requires either an obscene proposal or threat	
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.	1. May not apply to electronic communications. 2. May not apply when a cyberstalker dupes an "innocent" third party to harass.	1. Requires obscene proposal or 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. Requires a threat. 2. May not apply to electronic communications. 3. May not apply when a cyberstalker dupes an "innocent" third party to harass.

	Utah	Utah	Vermont	Vermont	Virginia
Code	UTAH CODE ANN. § 76-5-106.5 (West 2005).	UTAH CODE ANN. § 76-9-201 (West 2005).	VT. STAT. ANN. tit. 13, § 1061 (2005).	VT. STAT. ANN. tit. 13, § 1027 (2005).	VA. CODE ANN. § 18.2-152.7:1 (West 2005).
Title	Stalking	Electronic Communication Harassment	Stalking	Disturbing Peace by Use of Electronic Communication (misdemeanor)	Harassment by Computer (misdemeanor)
Reasonable Person Standard?	Yes, but requires a threat	No, but has standard where stalker insults, taunts, or challenges the recipient in a manner likely to provoke a violent or disorderly response	Yes	No	No, but broad harassment standard
Credible Threat Standard?	Yes visual or physical proximity to a person, or threats	Yes (one option; see "reasonable person standard")	No	Yes	Yes (one option; see "reasonable person standard")
Requires Actual Physical Pursuit?	Either physical pursuit or a threat	No	No	No	No
Statute Covers Electronic Communications?	Not specifically	Yes	Yes	Yes	Yes
Notes		Also prevents conduct that causes disruption, jamming, or overload of an electronic communication system through excessive message traffic of other means utilizing communication device.		May address e-mail bombs. *See* § 13-1027(a)(iii)	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.
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.	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 require obscene proposal or 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.	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.

Code	Virginia VA. CODE ANN. § 18.2-60.3 (West 2005).	Washington WASH. REV. CODE ANN. § 9.61.260 (West 2005).	Washington WASH. REV. CODE ANN. § 9A.46.110 (West 2005), *amended by* 2006 Wash. Legis. Serv. Page no. 2 (West).	Washington WASH. REV. CODE ANN. § 9A.46.020 (West 2005).	Washington WASH. REV. CODE ANN. § 9.61.230 (West 2005).
Title	Stalking	Cyberstalking	Stalking	Harassment	Telephone Harassment
Reasonable Person Standard?	Yes	No, but has broad harassment standard	Yes	No	No, but has broad harassment standard
Credible Threat Standard?	No	Yes (one option; see "reasonable person standard")	No	Yes	Yes (one option; see "reasonable person standard")
Requires Actual Physical Pursuit?	No	No	No	No	No
Statute Covers Electronic Communications?	Not specifically	Yes	Yes	Yes	No
Notes		May cover e-mail bombs. *See* § 9.61.260(1)(b).			
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. May not apply when a cyberstalker dupes an "innocent" third party to harass.	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).

	West Virginia	West Virginia	Wisconsin	Wisconsin	Wisconsin
Code	W. VA. CODE ANN. § 61-2-9a (LexisNexis 2005).	W. VA. CODE ANN. § 61-3C-14a (LexisNexis 2005).	WIS. STAT. ANN. § 940.32 (West 2005).	WIS. STAT. ANN. § 947.013 (West 2005).	WIS. STAT. ANN. § 947.0125 (West 2005).
Title	Stalking Harassment	Threatening Communications by Computer	Stalking	Harassment	Unlawful use of computerized communication systems (misdemeanor)
Reasonable Person Standard?	Yes *See* § 61-2-9a(g)(1)	No, uses broad harassment standard, but requires cyberstalker to contact victim	Yes, but requires direct contact with victim	No, but uses broad harassment standard	No, but uses broad harassment standard
Credible Threat Standard?	Yes (one option; see "physical pursuit")	Yes (one option)	No	Yes (one option; see "reasonable person standard")	Yes (one option; see "reasonable person standard")
Requires Actual Physical Pursuit?	Sometimes Requires following unless there is repeated harassing or credible threats	No	No	No	No
Statute Covers Electronic Communications?	Not specifically	Yes	Not specifically, but course of conduct includes sending material by any means to the victim	Not specifically	Yes
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 not apply when a cyberstalker dupes an "innocent" third party to harass.	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.

	Wyoming
Code	WYO. STAT. ANN. § 6-2-506 (2005).
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?	Yes
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

	FEDERAL CODE	FEDERAL CODE	FEDERAL CODE
Code	18 U.S.C. § 875(c) (2006)	47 U.S.C. § 223	18 U.S.C. § 2261A (2006)
Title	Interstate Communications Act	Federal Telephone Harassment Statute	Federal Interstate Stalking Punishment and Prevention Act
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	Yes
Notes			
Potential Statutory Problems	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. 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 when a cyberstalker dupes an "innocent" third party to harass.	1. May not apply when a cyberstalker dupes an "innocent" third party to harass.