

STORAGE NAME: h1759.it.doc

DATE: March 12, 2001

**HOUSE OF REPRESENTATIVES
COMMITTEE ON
INFORMATION TECHNOLOGY
ANALYSIS**

BILL #: HB 1759 (PCB IT 01-03)

RELATING TO: Cyberstalking

SPONSOR(S): Committee on Information Technology

TIED BILL(S):

ORIGINATING COMMITTEE(S)/COUNCIL(S)/COMMITTEE(S) OF REFERENCE:

- (1) INFORMATION TECHNOLOGY YEAS 11 NAYS 0
 - (2)
 - (3)
 - (4)
 - (5)
-

I. SUMMARY:

Cyberstalking, in general terms, is the use of the Internet, email, or other electronic communications to harass or threaten another person. Stalkers often use electronic media to stalk their victims because the stalkers can maintain anonymity. Recent studies indicate that cyberstalking is on the rise. Many states have either specific anti-cyberstalking statutes or stalking statutes that include harassment by electronic means as a form of stalking.

Although cyberstalking may fall within the conduct currently prohibited by Florida's stalking statute, s. 784.048, F.S., the Information Service Technology Development Task Force recommended that the statute be amended to specifically include cyberstalking within the scope of prohibited conduct. PCB IT 01-03 would implement this recommendation by defining the term "cyberstalk" and including cyberstalking within the prohibited conduct amounting to stalking or aggravated stalking.

PCB IT 01-03 would also amend s. 784.048 to widen the scope of threats that constitute stalking. Under the current language, only threats creating a reasonable fear of violence against the recipient of the threat constitute stalking. PCB IT 01-03 would amend this language to include threats creating a reasonable fear of violence or bodily injury to the recipient's child, sibling, spouse or dependent.

II. SUBSTANTIVE ANALYSIS:

A. DOES THE BILL SUPPORT THE FOLLOWING PRINCIPLES:

- | | | | |
|-----------------------------------|---|--|------------------------------|
| 1. <u>Less Government</u> | Yes <input type="checkbox"/> | No <input checked="" type="checkbox"/> | N/A <input type="checkbox"/> |
| 2. <u>Lower Taxes</u> | Yes <input type="checkbox"/> | No <input checked="" type="checkbox"/> | N/A <input type="checkbox"/> |
| 3. <u>Individual Freedom</u> | Yes <input type="checkbox"/> | No <input checked="" type="checkbox"/> | N/A <input type="checkbox"/> |
| 4. <u>Personal Responsibility</u> | Yes <input checked="" type="checkbox"/> | No <input type="checkbox"/> | N/A <input type="checkbox"/> |
| 5. <u>Family Empowerment</u> | Yes <input checked="" type="checkbox"/> | No <input type="checkbox"/> | N/A <input type="checkbox"/> |

For any principle that received a "no" above, please explain:

PCB IT 01-03 would probably increase the burdens on, and costs of operating, the criminal justice system due to increased prosecutions. PCB IT 01-03 would also restrain individual freedom to disseminate threats through the Internet, email or other electronic media.

B. PRESENT SITUATION:

The use of the Internet, email and other electronic communications devices to harass or threaten another person is commonly referred to as "cyberstalking." The widespread use of information technology has created a relatively anonymous mechanism for stalkers to annoy, harass and threaten victims. Instances of cyberstalking often escalate into real life stalking or other physical assaults.¹

In 1999, former Vice President Gore asked the Attorney General to study the problem of cyberstalking and to provide a report (the "Cyberstalking Report") containing recommendations on how to help protect people from cyberstalkers.² The Cyberstalking Report noted that many stalkers, including both online and offline stalkers, are motivated by a desire to exert control over their victims and that stalkers engage in similar conduct to accomplish their goals. In most cases, the cyberstalker and the victim had a prior relationship, and the cyberstalking began when the victim attempted to sever the relationship. Some victims were, however, cyberstalked by strangers.

As the Cyberstalking Report notes, "The fact that cyberstalking does not involve physical contact may create the misperception that it is more benign than physical stalking. This is not necessarily true." Although a potential stalker may be unwilling to directly confront a victim in person or on the telephone because of the fear that they may be recognized, the stalker may be less reluctant to send more anonymous electronic communications to a victim. Sophisticated cyberstalkers, for example, may utilize computer programs to send repeated messages to a victim even when the cyberstalker is not at his or her computer. After gaining a victim's personal information, such as the

¹ In the first successful prosecution under California's anti-cyberstalking law, a 50-year old former security officer pleaded guilty and was sentenced to six years in prison. The defendant terrorized his 28-year old victim by impersonating her in various chat rooms where he posted, along with her address and telephone number, messages that she fantasized about being raped. On at least six occasions, sometimes in the middle of the night, men knocked on the woman's door saying they wanted to rape her. See Gina Keating, Man Gets Life Sentence for Cyber Stalking of Woman He Met at Church, City News Service, July 22, 1999, available at LEXIS, New Library, City News Service file.

² See U.S. Dep't of Justice, 1999 Report on Cyberstalking: A New Challenge for Law Enforcement and Industry (August 1999), available at <http://www.usdoj.gov/criminal/cybercrime/cyberstalking.htm> (Last visited March 8, 2001) (hereinafter "Cyberstalking Report").

victim's email address, phone number or physical address, a cyberstalker may impersonate a victim in a chat room, post a controversial message, and elicit responses to be sent to the victim.

By using electronic media, cyberstalkers can maintain relative anonymity while stalking their victims. Cyberstalkers can use false information to obtain their email address or Internet Service Provider (ISP). Cyberstalkers can also use 'remailers,' or email systems that automatically forward a message, to cloak the source of their emails. A cyberstalker's anonymity creates an ominous fear in the victim's mind.

Although reliable data on the prevalence of cyberstalking is scarce, anecdotal evidence gathered by the United States Department of Justice suggests that cyberstalking is a growing problem. For instance, the Los Angeles District Attorney estimates that email or other electronic communications were a factor in approximately 20 percent of stalking cases. As the Cyberstalking Report indicates, "The Computer Investigations and Technology Unit of the New York City Police Department estimates that almost 40 percent of the caseload in the unit involves electronic threats and harassment...." ISPs are also receiving increased complaints from their users about instances of cyberstalking on their services. The Cyberstalking Report noted, however, that ISPs seldom respond to these complaints.

Most states have statutes making stalking illegal, and roughly half of the states have specific anti-cyberstalking statutes or anti-stalking statutes that cover electronic communications.³ Florida has a general anti-stalking statute, s. 784.048, F.S., but not a specific anti-cyberstalking statute.

Florida's anti-stalking statute creates two offenses: stalking and aggravated stalking. Subsection (2) provides that "Any person who willfully, maliciously and repeatedly follows or harasses another person commits the offense of stalking, a misdemeanor of the first degree." Subsection (3) provides that "Any person who willfully, maliciously, and repeatedly follows or harasses another person, and makes a credible threat, with the intent to place that person in reasonable fear of death or bodily injury, commits the offense of aggravated stalking, a felony of the third degree."

"Harass," as defined by s. 784.048, means to "engage in a course of conduct directed at a specific person that causes substantial emotional distress in such person and serves no legitimate purpose." When determining whether an incident created substantial emotional distress, as element of "harassment" under s. 784.048, courts ask whether a reasonable person would suffer substantial emotional distress as a result of the defendant's conduct. See *Bouters v. State*, 659 So.2d 235, 238 (Fla.1995). Although cyberstalking may fall within the broad definition of harassment, stalking has traditionally involved a physical proximity component, and existing laws may not be interpreted to address cyberstalking.

The Information Service Technology Development Task Force ("Task Force"), in its 2001 Report to the Legislature and Governor, recommended that s. 784.048 be clarified to specifically include cyberstalking within the purview of the statute.⁴ The Task Force suggested that s. 784.048 be amended to define cyberstalking to mean "the communication of words, images, or language by or through electronic mail or electronic communication that is directed at a specific person and that causes substantial emotional distress in such person and that serves no legitimate purpose."

³ See, e.g., ALASKA STAT. § 11.41.270 (Michie 2000); N.C. GEN. STAT. § 14-196.3 (West's 2000) (North Carolina); CAL. PENAL CODE § 646.9 (2000) (California); MASS. GEN. LAW ANN. ch. 265, § 43 (2000); N.H. REV. STAT. ANN. § 633:3-a, 644:4 (2000) (New Hampshire); OKLA. STAT. ANN. tit. 21, § 1173 (2000); PA. CONS. STAT. § 5504 (2000).

⁴ See 2001 Annual Report to the Legislature, Information Service Technology Development Task Force § 7.4.2, available at http://www.itflorida.com/pdfs/2001_legislative_report.pdf (February 14, 2001).

C. EFFECT OF PROPOSED CHANGES:

PCB IT 01-03 would amend s. 784.048, F.S., to define the term “cyberstalk” and would include cyberstalking within the conduct prohibited under the stalking statute. PCB IT 01-03 would create a new subsection (1)(d) to define the term “cyberstalk” consistent with the definition suggested by the Task Force. Under PCB IT 01-03, “cyberstalk” would be defined for the purposes of s. 784.048 to mean:

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, that causes substantial emotional distress in such person and serves no legitimate purpose.

The language “or cause to be communicated” is added to the definition to ensure that where a person is not the actual sender of the threat but caused the threats to be communicated to the victim, the person is also guilty of cyberstalking. Recent incidents involving a cyberstalker posing as the victim and initiating a barrage of threatening emails to the victim would be included within the offense.

The term ‘cyberstalk’ would also be inserted in subsection (2) and subsection (3) of s. 784.048 to be included in the prohibited conduct amounting to “stalking” or “aggravated stalking.”

Under the existing language of s. 784.048(3), only threats communicated to the recipient placing the recipient himself or herself in reasonable fear of death or bodily injury would constitute aggravated stalking. PCB IT 01-03 would broaden subsection (3) to include within the offense of aggravated stalking threats made by traditional stalkers or cyberstalkers that cause the recipient to reasonably fear death or bodily injury to the recipient’s child, sibling, spouse, or dependent. This expansion of the statute’s prohibition is consistent with changes to anti-stalking statutes made by other states to include threats against family members.⁵

Prosecution of cyberstalking may prove relatively more difficult for law enforcement than prosecution of other forms of stalking. The anonymity of a cyberstalker may make many instances of cyberstalking difficult to prosecute. However, PCB IT 01-03 would ensure the prosecution of cyberstalkers whose identities are discovered. As with any crime committed over the Internet or through other electronic means, law enforcement officers may face difficulties when investigating crimes committed by persons who reside in other states (i.e. cyberstalker in Montana and victim in Florida).⁶ As the Cyberstalking Report noted, law enforcement officials investigating cyberstalking have faced resistance from out-of-state law enforcement officials when the perpetrator resides in another state and the offense has not yet resulted in any physical violence to the victim.⁷ States faced with resistance from other states may refer reports of interstate cyberstalking to the FBI. Despite these difficulties, empirical evidence showing that most cyberstalkers actually know their victim indicates that where a victim lives in Florida, the cyberstalker probably does as well.

⁵ See, e.g., ALASKA STAT. § 11.41.270 (Michie 2000); ARK. CODE ANN. § 5-71-229 (Michie 2000); ME. REV. STAT. ANN. tit. 17, § 210-A (West 2000) (Maine); N.H. REV. STAT. ANN. § 633:3-a (2000) (New Hampshire); OKLA. STAT. ANN. tit. 21, § 1173 (2000); 18 PA. CONS. STAT. § 5504 (2000).

⁶ See Cyberstalking Report.

⁷ See Cyberstalking Report.

Thus, while jurisdictional concerns may arise in some cases, in many other cases, jurisdiction will not be an issue.

D. SECTION-BY-SECTION ANALYSIS:

This section need be completed only in the discretion of the Committee.

III. FISCAL ANALYSIS & ECONOMIC IMPACT STATEMENT:

A. FISCAL IMPACT ON STATE GOVERNMENT:

1. Revenues:

PCB IT 01-03 would generate no new revenues, except through the collection of any fine imposed as a criminal penalty for conviction of any prohibited act.

2. Expenditures:

PCB IT 01-03 would require the State to fund its proportionate share of the additional cost of investigating, prosecuting, convicting, incarcerating and supervising persons convicted of cyberstalking or aggravated stalking directed at a person's family members.

B. FISCAL IMPACT ON LOCAL GOVERNMENTS:

1. Revenues:

PCB IT 01-03 would generate no new revenues, except through collection of any fine imposed as a penalty for conviction of any prohibited act.

2. Expenditures:

PCB IT 01-03 would require local governments to fund their proportionate shares of the additional costs of investigating, prosecuting, convicting, incarcerating and supervising persons convicted of cyberstalking or aggravated stalking directed at a person's family members.

C. DIRECT ECONOMIC IMPACT ON PRIVATE SECTOR:

There is no reliable estimate of the impact that PCB IT 01-03 might have on the private sector.

D. FISCAL COMMENTS:

N/A

IV. CONSEQUENCES OF ARTICLE VII, SECTION 18 OF THE FLORIDA CONSTITUTION:

A. APPLICABILITY OF THE MANDATES PROVISION:

PCB IT 01-03 is expressly excepted from analysis under this part because it would be a criminal law.

B. REDUCTION OF REVENUE RAISING AUTHORITY:

PCB IT 01-03 is expressly excepted from analysis under this part because it would be a criminal law.

C. REDUCTION OF STATE TAX SHARED WITH COUNTIES AND MUNICIPALITIES:

PCB IT 01-03 is expressly excepted from analysis under this part because it would be a criminal law.

V. COMMENTS:

A. CONSTITUTIONAL ISSUES:

Any time the state attempts to regulate speech, concerns about the First Amendment and overbreadth arise. As the Cyberstalking Report noted, anti-stalking statutes must be necessarily broad to encompass a wide range of harassing communications. Because anti-stalking statutes can involve expressive conduct and speech, anti-stalking statutes must be carefully drafted so as not to impinge upon protected speech. Caution is particularly appropriate with regard to anti-cyberstalking statutes, because the Internet has been recognized as an important forum for protected speech. See *Reno v. ACLU*, 521 U.S. 844, 850-52 (1997).

However, the United States Supreme Court has stated that the government may criminalize credible threats without violating the First Amendment. See *Watts v. United States*, 394 U.S. 705 (1969). The Florida Supreme Court has also held that the existing language in s. 784.048 does not violate the First Amendment. See *Bouters v. State*, 659 So. 2d 235, 237 (Fla. 1995). Because PCB IT 01-03 requires that, to be considered cyberstalking, the communication must cause substantial emotional distress to the recipient of the threat, cyberstalking may be criminalized consistent with the First Amendment.

B. RULE-MAKING AUTHORITY:

PCB IT 01-03 does not confer rule-making authority on any government entity.

C. OTHER COMMENTS:

N/A

VI. AMENDMENTS OR COMMITTEE SUBSTITUTE CHANGES:

N/A

VII. SIGNATURES:

COMMITTEE ON INFORMATION TECHNOLOGY:

Prepared by:

Staff Director:

Richard Martin

Charles Davidson