

Portland State University

**PDXScholar**

---

Criminology and Criminal Justice Senior  
Capstone Project

Criminology and Criminal Justice

---

Winter 2012

# Prevention of Cyberstalking: A Review of the Literature

Portland State University. Criminology and Criminal Justice Senior Capstone

Follow this and additional works at: [https://pdxscholar.library.pdx.edu/ccj\\_capstone](https://pdxscholar.library.pdx.edu/ccj_capstone)



Part of the [Criminology and Criminal Justice Commons](#)

**Let us know how access to this document benefits you.**

---

## Recommended Citation

Portland State University. Criminology and Criminal Justice Senior Capstone, "Prevention of Cyberstalking: A Review of the Literature" (2012). *Criminology and Criminal Justice Senior Capstone Project*. 1.

[https://pdxscholar.library.pdx.edu/ccj\\_capstone/1](https://pdxscholar.library.pdx.edu/ccj_capstone/1)

This Technical Report is brought to you for free and open access. It has been accepted for inclusion in Criminology and Criminal Justice Senior Capstone Project by an authorized administrator of PDXScholar. Please contact us if we can make this document more accessible: [pdxscholar@pdx.edu](mailto:pdxscholar@pdx.edu).

# Prevention of Cyberstalking:

A Review of the  
Literature

Portland State University

Winter 2012 Criminology and Criminal Justice Senior Capstone Class:

Michael Abshier, Kerry Allen, Kelly Anderson, Brandon Awbrey, Stephen Brown, Michael Davis, Francina Den Arend, Joshua Greenwalt, Amy Hinson, Jerry Martinez, David Millenaar, Eric Morse, Brittany Morton, Rachel Niten, Amina Oleiwan, Kelly Peterson, Christopher Pitchford, Richard Ramos, Joseph Russau, Elizabeth Schiemer, Valarie Shepherd, Adam Spang, David Stefanini, Lisa Storelli, Jennifer Trueman, Jesse Vinavong

Supervised by: Dr. Debra Lindberg

## Table of Contents

Introduction.....	3
Definition and Prevalence.....	3
Victims.....	4
Offenders.....	<b>Error! Bookmark not defined.</b>
Modus Operandi.....	7
Prevention.....	8
Conclusion.....	9
References.....	<b>Error! Bookmark not defined.</b>

## Introduction

With technological advances and increases in the number of people who can access and use technology, cyberstalking is a crime increasing in prevalence across the United States. The goal of this report is to provide a more clear understanding of the definition of cyberstalking, its prevalence, characteristics of both the victims and offenders of this crime, and the modus operandi of the crime. In addition, potential strategies to prevent cyberstalking will be discussed, including but not limited to changing internet behavior and educating the public about cyberstalking.

## Definitions and Prevalence

Nine of the articles reviewed explicitly defined cyberstalking. These articles also contained data on the prevalence of cyberstalking in the United States, Finland, and Great Britain.

Stalking can be defined as recurring unwelcome attention which causes people to fear for their own safety and for the safety of those closest to them (Baum, Catalano, Rand, & Rose, 2009, p.1). In British culture, the term, “harassment,” is used interchangeably with, “stalking,” and is considered the act of an individual consistently attempting to gain the attention of another through a variety of threatening means whereby victims become fearful and concerned for their safety (Wykes, 2007, p.158).

Cyberstalking occurs when an individual is harassed through computer technology and the use of local area networks connected to the internet (Reyns, Henson, & Fisher, 2011, p.1153).

Stambaugh, Beaupre, Baker, Cassaday, and Williams (2000, p.1) define cyberstalking as an electronic crime involving a perpetrator using the internet or other high tech communication devices to take advantage of systematic weaknesses, or to exploit a person’s vulnerability, including stalking a person online.

By definition, any cybercrime may only be committed through the misuse of electronic devices, specifically those which have the capability of internet services. Any of the following categories may constitute the perpetration of cyberstalking: persistent unwanted contact, repeated unwanted harassment, persistent and unwanted sexual advances, or implied threats or acts of violence (Reyns et al., 2011). In one study of 974 participants of potential stalking crimes, 41% were victims of cyberstalking as described by one or more of the four definitions. Of the 41%, 23% were victims of unwanted contact, 20% of harassment, and 14% experienced unwanted sexual advances and 4% were threatened with acts violence (Reyns et al., 2011).

Cyberstalking occurs frequently among college students in the United States and European countries (Bjorklund, Hakkanen-Nyholm, Sheridan, & Roberts, 2010; Finn, 2004; Henson, Reyns, & Fisher, 2011). At a large urban university in the Midwestern United States, 42% of the

students who used online social network sites admitted to being victims of cyberstalking (Henson et al., 2011, p.254). In a similar study conducted among Finnish college students, 48% were subjected to stalking or unwanted behavior (Bjorklund et al., 2010, p.689).

Overall, it is predicted nearly one in every five people will become a victim of stalking in their lifetimes, and women are almost two and a half times more likely than men to be victims (Spitzberg, 2002, p.266). In a meta-analysis of 103 research studies of stalking related incidents involving 70,000 individuals, approximately three fourths of the perpetrators had some type of relationship with the victims and nearly half of all occurrences occurred between past romantic partners (Spitzberg, 2002, p.263). A longitudinal study of 82 women in New York City that examined the relationship between stalkers and their victims found 84% of stalkers were past partners (Cattaneo, Cho, & Botuck, 2011, p.3437). Logan and Walker (2009) state partner stalking can be defined as being followed, threatened, or harassed during an intimate relationship or after the relationship has ended (p.265). The same researchers found partner stalking can be considered different from other types of stalking such as acquaintance and stranger stalking, as the consequences are greater for victims of partner stalking because of the physical dominance and harmful nature of the former relationship (p.263).

## **Victims**

Our research led us to 11 articles describing common characteristics of cyberstalking victims. As internet and telecommunication technologies advance, the threat of becoming a cyberstalking victim increases. Applicable findings from studies conducted in the United States and Finland about victims of cyberstalking are discussed below.

Several authors discussed the ways in which internet usage may influence victimization. Stalkers often use the internet to send unwanted emails and messages to victims (Finn, 2004, p.468). Fox (2001, p.264) explained that many people volunteer personal information to organizations for the sake of convenience (e.g., banking and retail membership discount cards), thus leaving the internet “door” open for would-be offenders who keep track of a victim’s routine activities by monitoring their online behaviors (Van Wilsem, 2011, p.117). In most stalking cases, the victim knows his/her stalker and the majority of the relationships are either current or ex-intimate (Cattaneo et al., 2011, p.3429). Wykes (2007) notes the relationship between our culture’s focus on appearance and wealth and the phenomenon of cyberstalking. The abundance of personal information online, including celebrity web pages, has blurred the lines between unapproachable and accessible, increasing the occurrence of cyberstalking victimization, including celebrity victims and media icons (p.170).

There are also many attributes of today’s technology which have increased the risk of being a victim of cyberstalking. Van Wilsem (2011) notes greater use of technology and online tools for communication including webcams, chat rooms, social media, and online dating sites enhance

the level of transparency a person has in the digital world (p.117). This exposes vulnerabilities and potentially affects the likelihood a victim may cross paths with a perpetrator. Other factors increasing the chance of victimization include the frequency of updating one's account (of any type) and adding strangers as friends (Henson et al, 2011, p.260) and the use of chat rooms, regardless of the gender of the victim (Marcum, Ricketts, & Higgins 2010, p.420).

Reyns et al (2011) reported a predictor of becoming a victim of cyberstalking was the victim's past deviant internet behavior, which included downloading pirated media, contacting someone in a threatening manner, and sending sexual images. Individuals who engaged in deviant online behavior were found to be 14 times more likely to be victims of cyberstalking. It is not surprising that not engaging in deviant online activities reduced the chance of victimization (p.1163).

Several studies discovered females were more likely to be cyberstalking victims. A Finnish University survey of students discovered nearly 50% of respondents had been stalked at least once (Bjorklund et al, 2010, p.684). Another study reported 52.4% of cyberstalking victims were females, while another found women were stalked two and a half times more frequently than men (Reyns et al., 2011, p.1155, Baum et al., 2009; Henson et al, 2011; Spitzberg (2002, p.262).

## Offenders

A review of 12 articles revealed information regarding offenders of the crime of cyberstalking. These included offender characteristics as well as factors associated with carrying out the crime. The findings are described below.

Several studies identified characteristics related to the age, gender, and ethnicity of stalking offenders. They are mainly (59.7%) between the ages of 19 and 30 (Bjorklund et al, 2010, p.689). Studies varied in determining the gender of most stalkers. One study estimates 91.8% of offenders are men (Bjorklund et al., 2010, p.689). Another survey, however, reported more complicated scenarios: When a victim was male, the offender was also male 41.3% of the time, female 42.5% of the time, and unknown 16.1% of the time; when a victim was a female; the offender was male 66.9% of the time, female 23.5% of the time, and unknown 9.3% of the time. The same researchers also found most offenders stalked victims of the same ethnicity and that nearly 83% of Caucasian victims were stalked by Caucasians, while 66% of African Americans identified their perpetrator as being of the same ethnicity (Baum et al, 2009, p.4).

Other studies focused on the stalker's demeanor and mental characteristics. Testimonies from stalking victims consistently revealed how personable, caring, and charismatic offenders seemed at first, but how those initially appealing features quickly transformed. Once an offender had won over his/her victim, however, the need to control emerged and behavior including outward acts of jealousy, aggression and threats, and mental abuse was displayed (Cox & Speziale, 2009, pp.8-9). Mental characteristics of offenders include a tendency to display low to medium mental

impairment when entering the criminal justice system (Prins, 2005, p.351), as well as nonconforming psychological states of being and antisocial behaviors (Kamphuis & Emmelkamp, 2005, p.170).

Some articles addressed reasons for cyberstalking. An overwhelming number of victims (75%) were stalked by a known person, most commonly a neighbor, co-inhabitant, or past romantic partner/companion (Baum et al, 2009, p.4). Spitzberg (2002, p.278) found most stalking started after a relationship between known parties ended, but Logan and Walker suggest cyberstalking begins during a relationship and continues, even after it's termination, the stalker using his/her intimate knowledge of the victim's personal life as an aid in commission of the crime (2009, pp.252-253). Ill will, rage, and revenge were the most frequent reasons victims listed for being stalked by a person known to them and nearly 17% thought the stalker was trying to maintain the connection (Baum et al, 2009, p.5).

Cyberstalkers maintain their anonymity by using internet technologies to conceal their actions (Wykes, 2007; Harrison, 2006). One study reported some offenders hacked computers to secretly monitor their victim's activities (Cox & Speziale (2009, p.9). Another study found 22 out of 82 women stated they had received unwelcome, anonymous emails, written messages, or other commentary (Cattaneo et al. 2011, p.3441).

Cyberstalking has been connected to pedophilia. Kohm and Greenhill (2011, p.198) defined a pedophile as an adult who finds prepubescent children sexually attractive and seeks out their attention. Of adults to stalk children on the internet, 74% were 20-49 years old and 95% were males (Alexy, Burgess, & Baker 2005, p. 805-806). Wykes notes children are easy victims for pedophile cyberstalkers, as they are more readily taken in by trickery and manipulation (2007, p.168).

## **Modus Operandi**

A review of nine articles provided illuminating information on offenders' *modi operandi* (M.O.s) related to stalking their victims. Much of the information provided focused on internet use.

Spitzberg (2002) described several types of stalking typology. One type is hyper-intimacy, where the victim receives gifts, letters, persistent calls, emails, and personal contact. Another typology is pursuit and proximity, where the offender follows and conducts surveillance on a victim. Invasion tactics are described as instances where the offender breaks into the victim's residence and takes personal property. Offenders may also take a role of intimidating and harassing victims by tarnishing their reputations and sending intimidating letters or emails. Coercion and constraint might also be used to restrict the behavior of victims (e.g., kidnapping and imprisonment). The last typology is the use of aggression (i.e., force and rage towards a victim resulting in injury or death) (p.269).

Other studies described stalkers' various methodologies. Some stalkers try to obtain information about their victims indirectly, either by contacting family, friends, or acquaintances, or by sending messages, flowers, gifts, and other forms of unwanted correspondence. Others may try to stalk their victims directly by making contact over the phone or face to face meetings (Baum et al., 2009; Cattaneo et al., 2011, p.3440; Cox & Speziale, 2009, p.9).

Technology has provided stalkers with a new and unique set of tools to gather information about their victims. According to Van Wilsem (2011, p.124) and Wykes (2007, p.167) stalkers often take advantage of the personal information stored on network sites, hard drives of personal computers, laptops, and smart phones to learn more about their victims. Some of the more industrious cyberstalkers also collect personal information about their victims through the use of hardware devices installed on the victim's computer to monitor key strokes, which enable the collection of passwords, PIN numbers, email accounts, and other personal information. Cyberstalkers may also use spyware software, which is available free over the internet or for purchase. Spyware allows a person anonymously to monitor the internet activity and habits of a target (Cox & Speziale 2009; Southworth, Finn, Dawson, Fraser, & Tucker, 2007, p.848; Reysn, et al., 2011; Wykes, 2007). Stalkers have also been known to use college campus computers and their internal networks to commit their cybercrimes (Peak, Barthe, & Garcia, 2008, p.257).

## Prevention Strategies

A review of 12 research articles found information on cyberstalking prevention strategies. These strategies included information about victim internet usage, victimization research and education, legal policies, and enforcement practices.

The first step to prevention is often education. Stambaugh, et al, (2000) note there is a need for increased public awareness of cyber-stalking. By making the public more aware of the problem, agencies at the local and federal levels may become more focused on preventative measures, which could, in turn, trigger multi-agency awareness campaigns (Baum et al., 2009).

Experts agree the best way to prevent becoming a cyberstalking victim is to become educated about these crimes and to seek professional assistance from law enforcement personnel and other agencies should it be suspected a cybercrime has occurred (Cox & Speziale, 2009, p.16). Victim advocacy, support organizations, prosecutors' offices are available to help prevent or reduce cyberstalking (Cox & Speziale, 2009, p.16; Southworth et al., 2007, pp.851-852). Cattaneo et al. (2011, p. 3446) found victims with protection orders had a 35.3% reduction in the stalking behavior and 15.4% reported it had stopped, altogether. It is also imperative that law enforcement personnel be well informed and supportive of stalking victims. Victims who believe they are being stalked should record all contacts with the offender, so as to be able to make reports which can be verified (Cox & Speziale, 2009, p.16; Miller & Smolter, 2011).



Prevention, however, cannot be left solely in the hands of law enforcement personnel and there are specific steps members of the community can take to reduce their risk of victimization. If juveniles refrain from conversing online with strangers, they reduce their odds of being victims. Juveniles should use caution when deciding to engage in online communication with unknown persons, especially if they are willing to divulge their personal information. It is highly recommended that youths become educated about the dangers of online communication and adults (most likely parents and teachers) should develop simple guidelines for youths online etiquette prior to initial internet use (Marcum et al., 2010, p.426).

Social networking sites can also contribute to becoming victims of cyberstalking. To prevent instances of cyberstalking, individuals should educate themselves on internet security measures and use these techniques to help control access to their personal information on sites such as Facebook and Myspace (Henson et al., 2011). Users should also avoid social networking activities which bring people in closer virtual contact such as adding strangers as friends, engaging in deviant activities (e.g., surfing sites depicting pornographic images), and associating online with deviant peers, all of which increase the likelihood of becoming victims of cyberstalking (Reyns et al., 2011).

Legislative and enforcement strategies may also help prevent cyberstalking. Deterrence approaches included the use of increased penalties to battle the growing problems of child exploitation and cybercrimes (Harrison, 2006, p.373). Mitchell, Wolak, and Finkelhor (2005) suggest law enforcement agencies initiate and take charge of internet investigations involving children in order to prevent crimes from occurring. This approach should include undercover investigations consisting of an officer impersonating a potential victim, particularly a minor. Collection of this evidence could serve as grounds for arrest of an offender and establish a record for him/her in the criminal justice system. This type of criminal sanction could deter future crimes due to the fear of law enforcement watching and enforcing unlawful internet communications (p.262). Stambaugh et al. (2000, p.3) states laws should be enacted to keep up with the evolution of technology.

## **Conclusion**

It is important to conduct further and continuing research on cyberstalking to help law enforcement and victim service providers build prevention strategies. Logan and Walker suggest qualitative research is needed to more completely understand the impact of cyberstalking on a victim's life, including monetary losses due to legal assistance, emotional damage, being fired from a job due to stalker interference, and family problems resulting from the time devoted solely to ending the stalking. Researching and validating these consequences will likely help society develop policies which actually prevent stalking, rather than trying to heal it later (2009, pp.264-265).

## References

- Alexy, E. M., Burgess, A. W., & Baker, T. (2005). Internet offenders. *Journal of Interpersonal Violence, 20*(7), 804-812.
- Baum, K., Catalano, S., Rand, M., & Rose, K. (2009). Stalking victimization in the United States. U.S. Department of Justice, Office of Justice Programs, Bureau of Justice Statistics. (NCJ 224527). Retrieved from U.S. Government website: <http://bjs.ojp.usdoj.gov/index.cfm?ty=pbdetail&iid=1211>
- Bjorklund, K., Hakkanen-Nyholm, H., Sheridan, L., & Roberts, K. (2010). The prevalence of stalking among Finnish university students. *Journal of Interpersonal Violence, 25*(4), 684-698.
- Cattaneo, L., Cho, S., & Botuck, S. (2011). Describing intimate partner stalking over time. *Journal of Interpersonal Violence, 26*(17), 3428-3454.
- Cox, L., & Speziale, B. (2009). Survivors of stalking. *Affilia, 24*(1), 5-18.
- Finn, J. (2004). A survey of online harassment at a university campus. *Journal of Interpersonal Violence, 19*(4), 468-483.
- Fox, R. (2001). Someone to watch over us: *Criminology and Criminal Justice, 1*(3), 251-276.
- Harrison, C. (2006). Cyberspace and child abuse images. *Affilia, 21*(4), 365-379.
- Henson, B., Reynolds, B. W., & Fisher, B. S. (2011). Security in the 21st century. *Criminal Justice Review, 36*(3), 253-268.
- Kamphuis, J. H., & Emmelkamp, P. M. G. (2005). 20 years of research into violence and trauma. *Journal of Interpersonal Violence, 20*(2), 167-174.
- Kohm, S. A., & Greenhill, P. (2011). Pedophile crime films as popular criminology: A problem of justice? *Theoretical Criminology, 15*(2), 195-215.
- Logan, T., & Walker, R. (2009). Partner stalking. *Trauma, Violence, & Abuse, 10*(3), 247-270.
- Marcum, C. D., Ricketts, M. L., & Higgins, G. E. (2010). Assessing sex experiences of online victimization: An examination of adolescent online behaviors using routine activity theory. *Criminal Justice Review, 35*(4), 412-437.

- Miller, S. L., & Smolter, N. L. (2011). "Paper abuse": When all else fails, batterers use procedural stalking. *Violence against Women, 17*(5), 637-650.
- Mitchell, K. J., Wolak, J., & Finkelhor, D. (2005). Police posing as juveniles online to catch sex offenders: Is it working? *Sexual Abuse: A Journal of Research and Treatment, 17*(3), 241-267.
- Peak, K. J., Barthe, E. P., & Garcia, A. (2008). Campus policing in America. *Police Quarterly, 11*(2), 239-260.
- Prins, H. (2005). Mental disorder and violent crime: A problematic relationship. *Probation Journal, 52*(4), 333-357.
- Reyns, B. W., Henson, B., & Fisher, B. S. (2011). Being pursued online: Applying cyberlifestyle – routine activities theory to cyberstalking victimization. *Criminal Justice and Behavior, 38*(11), 1149-1169.
- Southworth, C., Finn, J., Dawson, S., Fraser, C., & Tucker, S. (2007). Intimate partner violence, technology, and stalking. *Violence against Women, 13*(8), 842-856.
- Spitzberg, B. H. (2002). The tactical topography of stalking victimization and management. *Trauma, Violence, & Abuse, 3*(4), 261-288.
- Stambaugh, H., Beaupre, D., Icove, D., Baker, R., Cassaday, W., & Williams, W. (2000). *State and local law enforcement needs to combat electronic crime*. U.S. Department of Justice, Office of Justice Programs, National Institute of Justice. Retrieved from U.S. Government website: <https://www.ncjrs.gov/pdffiles1/nij/183451.pdf>.
- Van Wilsem, J. (2011). Worlds tied together? Online and non-domestic routine activities and their impact on digital and traditional threat victimization. *European Journal of Criminology, 8*(2), 115-127.
- Wykes, M. (2007). Constructing crime: Culture, stalking, celebrity and cyber. *Crime, Media, Culture, 3*(2), 158-174.