

Cyber Stalking - An Old Behavior ... A New Crime

National Conference on Health & Domestic Violence
Family Violence Prevention Fund
October 10, 2009, New Orleans, LA

Susan M. Hadley, MPH

Founder of WomanKind:
An Integrated Model of 24-Hour Health Response to Domestic Violence

Adjunct Faculty: University of Minnesota Medical School,

Doctoral Program: Fielding Graduate University
Media (Forensic) Psychology

Definition

- To understand scope of cyber stalking, important to understand concept of stalking
- Stalking, commonly defined as "*the willful, malicious and repeated following or harassing of another person*" is gaining recognition and validity as a serious crime in United States

(downloaded on 1.25.09 from www.ncvc.org)

Stalking Victimization in the United States

- Largest set of data on stalking prevalence and behavior to date found 3.4 million persons identified themselves as victims of stalking in a 12-month period

• *Stalking Victimization in the US* (Leary, ML, 2009, Stalking Resource Center.)

• Downloaded on 1.25.09 from www.ncvc.com.

Another Definition

- › Stalking ... which may be defined as a
- › “*course of conduct directed at a specific person ...*
- › *with repeated visual or physical proximity,*
- › *non-consensual communication,*
- › *verbal, written or implied threats, or combination that requires victims feel **high level of fear of bodily harm**” .*

(National Criminal Justice Association, 1993).

History of Legislation

- › Victims of IPV have long known about stalking
- › “Real life stalking” legislation in 1990s in California
 - Before this, law enforcement was powerless to act unless physical assault occurred; **See below**. Old habits die hard.
- › Michigan law included online communications

Note: Many present-day stalking victims still advised nothing can be done unless physical assault occurs

History of Legislation

- › As of September, 1993, all 50 states and DC have some form of stalking law; urgent need exists for model code
- › Consistency enhanced when US Congress passed the federal stalking law
- › In 2006, federal anti-cyber stalking law passed

- › Note: In some states, cyber stalking laws meant to protect victims under age of 18, not meant to be / and are not effective in broad population

Cyber Stalking

- ▶ Stalking with a technology component
 - Donovan & Bernier, 2009

Goals of Cyber Stalking

- ▶ To intimidate and induce fear in victim
- ▶ Donovan and Bernier (2009, p. 3) want to share:
 - Tools of cyber criminals
 - Explain how cyber stalkers think
 - Their goal: *"to put you (the victim) inside the head of someone who derives devious pleasure in proving he is smarter than his victim and in controlling his victim"*

Aggravated Stalking

- ▶ Michigan has passed statute addressing more serious stalking – Aggravated Stalking
 - Section 28.643(9) Definitions. 1993. Section 411i
- ▶ Adds presence of **physical threats** as aggravating factors in stalking
- ▶ *"Credible threat" means a **threat to kill** another individual or a **threat to inflict physical injury** upon another individual ... that causes individual hearing or receiving thereof to **reasonably fear for his or her safety** or safety of another individual*

Cyber Stalking Facts

- 66 % of stalkers pursue their victim once a week
- 78 % of stalkers use more than one approach.
- 81% of victims stalked by an intimate partner reported previously assaulted by that partner.
- 87 % of stalkers are men.

More Cyber Stalking Facts

- 94% of stalkers of female victims stalked by men.
- 60% of male victims are stalked by other men.
- 62 of cyber stalking victims are female, primarily ages 18-24". (Donovan, F. & Bernier, K., 2009).
(www.wiredsafety.org/resources/powerpoint/cyber_stalking_study.ppt)

IPV and Violations of OFPs

- Restraining orders or OFPs traditionally the only means of protection for stalking victims
- Rarely effective, with inconsistent enforcement
- Discipline perpetrators **after** orders violated
- Harm designed to protect has already occurred

Technologies Location & Surveillance

- › Global Positioning Systems
- › Cameras – Hidden and Not-So-Hidden
- › Cell Telephones, Caller ID, Fax Machines
- › Computer and Internet Technology
- › Computer Key Stroke and Key Logging Stalking
- › Internet, EMAIL ...
- › TTY / TTD

Mechanisms & Method Location and Surveillance Technologies

- › In past, abusers would check car odometers to monitor mileage and activities
- › Location-based services provided by cell phone carriers allow abuser to track victim's location
- › Enable abuser to precisely locate their victim

Global Positioning Systems

- › GPS use satellite receivers to provide precise real-time worldwide positioning
- › Variety of price, size and appearance from small black box, portable hand-held unit, tiny micro chip in wristband
- › Can even be activated remotely
- › When you purchase cell phone today; likely have feature (can turn on/off) to broadcast area you are calling from
- › Could be used by stalker to determine victim's location

Mechanisms & Methods Cameras

- ▶ Small wireless high-resolution cameras easily hidden ins smoke detectors, children's lamps or behind pin-sized hole in a wall

Mechanisms & Methods Telephone

- ▶ Repeated and harassing phone calls with threatening messages left on voice mail and answering machines
 - Verizon store
 - Use of prepaid calling card or prepaid cell phones;
 - If not activated with credit card or billed to individual's long distance phone carrier, intrusive call hard to trace

Mechanisms & Methods Caller ID

- ▶ Much activism concerning Caller ID
- ▶ Abuser comes home, checks Caller ID to uncover calls made during day

Mechanisms & Methods: Cellular & Wireless Telephones

- ▶ Stalkers monitor victims cell phone use through call history or billing records
- ▶ Cell phones offer variety to services permit abuser to maintain constant access
 - Phone-based instant messaging
 - Text messaging
 - Pagers

Mechanisms & Methods TTY/TTD

- ▶ Text based telephone record and save exact history of phone conversations
- ▶ Abusers have been known to impersonate victims by using TTY to seek information about her activities, work support system and/or location

Mechanisms & Methods: Fax Machines

- ▶ Fax header can be a "goldmine" for abuser/stalker
- ▶ Must remove the header
 - i.e. victim sends a fax from shelter to her attorney
 - who then faxes document to abuser's attorney
 - who gives papers to his client, the abuser.

Computers and the Internet

Internet and EMAIL

- Stalking via email signifies closest parallel to traditional stalking patterns, since most common forms of stalking behavior are by using telephone and sending mail
- Sending unwelcome email one of **most common** forms of stalking, including hate, obscene or threatening email.
- Sending **high volumes** of electronic junk mail/spamming
- Telemarketing solicitations not necessarily stalking
- It is **Manner** in which emails sent that constitutes stalking
 - Repetitively sent, designed to intimidate, cause fear ... include "*concerning behaviors*" and considered to be stalking

Computer Key Stroke Stalking

- Easy to accomplish, especially for motivated stalker
- Stalker can install a key-logging program on partner's computer, before end of relationship, free on Internet
- Records every keystroke partner makes
- Records passwords to every account of partner
- Mechanism for unauthorized use of online purchases with partner's credit cards

Windows Computers

- An individual Windows-based computer connected to Internet can be identified and connected to another computer also connected to the Internet (Ogilvie, 2000))
- The "connection" is a direct computer-to-computer connection allowing interloper to exercise control over computer to reach his target (not typical Internet interaction)
- Instructions on how to use technologies available on Internet for anyone with technology expertise & motivation

Computer Thumb Drive

- Snoopstick ... USB drive, like flash drives to carry data
- Drive launches secret program to allow someone to view everything typed on target computer from any other computer in the world
- Consider possibilities for this tool
- Marketed as parental control tool with ability to block access to websites or restrict access to target computer during certain hours (Donovan & Bernier, 2009)

Abusers are Motivated

- Abusers and stalkers often highly motivated
- Use free and fee-based websites to track private information about victims
- Commercial entities, called information brokers, buy/sell data; information from public records / retail databases.
- Free websites, i.e. court databases, voter registration and religious directories make available private contact information to track survivors all over country

- ▶ When offenders know they are monitored, along with swift sanctions for violations, they can contain their behaviors. (Dunne, 2009)

An Essential Task

- ▶ **Task:** Raising the level of awareness and educating policy makers
- ▶ Rapidly increasing technology speaks a vastly different language than the language spoken within the older, traditional criminality.

A "Strong & Urgent" Warning

- ▶ Donavon and Bernier (2009) send a strong and urgent warning to current or potential victims when they say that just like domestic violence, stalking and cyber stalking at the hands of a current or former intimate partner, **can escalate and result in imminent danger or death to a victim.**

Danger Potential

Danger potential increased in "dramatic moments"

- when a victim tries to leave the abuser
- arrest of the perpetrator
- issuance of a protection
- restraining or stalking order
- court or custody hearings
- anniversary dates or any family-oriented holiday.

Safe Use of Technology

Using GPS To Stop Violence

- Tracking perpetrators wearing ankle bracelets
- In 2008, 30% of OFPs violated in Minnesota: 3,119 of 10,798
 - Only 100 have been locked up in Minnesota for violating OFPs
 - Cost of paying for program seen as issue
 - Cheaper than jail: Device cost: \$25/day vs. \$75/day for jail

3-Year Study - Newburyport, MA

- 14 offenders wore GPS-tracking bracelets for 3 years
- No domestic homicides in target area; incidents tripled rest of MA
- Civil rights advocates challenged GPS tracking saying it infringes on rights of abusers who never violate OFPs

Technology – Keeping Victims Safe

- NNEDV Safety Net project, launched in 2002
- Sees technology as a tool for survivors
- Intimate partner stalking NOT a new phenomenon
- BUT, continuing advancement of technology is providing stalkers with increasingly complex arsenal of tools
- Technology Safety Training-the-Trainers program, 2008
 - Cindy Southworth, Director of NNEDV's Safety Net project
 - Sponsors: Verizon *Hopeline* & Foundation, Mary Kay Ash, Symantec, AOL, Google & Loopt

Technology - Keeping Victims Safe

WCADV, Technology Safety Program

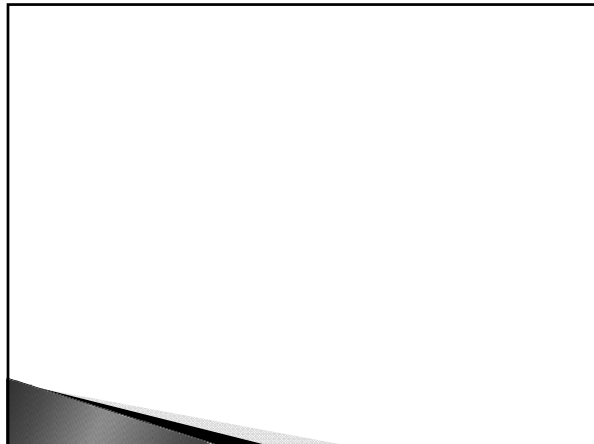
- ▶ IPV is built around control; abuser tries to limit woman's access to information & support
- ▶ Shelter – Internet, Email exchanges, cell phones, GPS
 - ▶ "Key stroke logger" on computer-intercept & read email
- ▶ Illustrate ways women might be monitored, i.e. abuser might search for children via social networking sites in order to find their mother.
- ▶ Become knowledgeable of the **safe use of technology** to minimize risk and keep personal information safer

Tips for Victims

- ▶ Always check for GPS – **Always**.

Tips for Victims (cont)

- ▶ Safety planning





Questions to Consider

- Have internet-based and electronic technologies created **new types of crime** requiring new legislative, law enforcement and legal responses;
- Or are these crimes simply **new expressions of traditional crimes i.e. new mechanisms & methods.** requiring simple adaptation of current legislative and law enforcement strategies?

Discussion and Answer ?

- Cyber stalking seems to entail broad character of traditional stalking, BUT in being **transposed** into virtual (electronic) environment, it is fundamentally **transformed** (Ogilvie, 2000, p. 2)
- Ogilvie believes before understanding nature of cyber stalking, must understand nature of **Internet**.

More Discussion

- Ogilvie concludes "*our attempts to protect the wider community from cyber crimes are hindered by failure on part of policy makers to appreciate that the Internet offers access to domains beyond the reach of traditional legislative frameworks*".
- Consider the considerable task of educating and generating technologically savvy policy makers
(Ogilvie, 2000, The Internet and Cyberstalking, p. 2)
