


**CYBER STALKING: DANGERS
LURKING ON THE INTERNET**

MALLIGA BATTAR, Ph.D
&
ROBERT KNAPTON, Senior Deputy
San Mateo County Sheriff's Office

CYBER STALKING



GENERAL OVERVIEW- I

- **What is cyber stalking?**
- **Different types of stalkers**
- **Different motivators**
- **A comparison of Online Vs. Offline stalking**
- **Typology of cyber stalking**
- **Anonymous services**
- **Mental illness and cyber stalking**
- **Psychopathic stalkers**

GENERAL OVERVIEW- II

- Federal Cyber stalking laws
- California State Cyber stalking laws
- Law enforcement response
- Specialized trained units
- Effects of social networking sites
- Do's and Don'ts of Internet romance
- General public recommendations
- Different relevant videos
- References

WHAT IS CYBER STALKING? - I

- Use of the internet, e-mail, or any other electronic communications to stalk another person
- Stalking usually involves harassing or threatening behavior in a repeated manner such as following a person, appearing at a person's (victim's) place, or business place
- Stalkers usually make harassing phone calls, leave written messages or objects, or vandalize a person's property

WHAT IS CYBER STALKING? - II

- Cyber stalkers meet or target their victims by using different search engines, bulletin and discussion boards, and online forums
- Cyber stalkers use different social network sites and self publishing media such as Face book, Twitter, Friendster, Bebo, Myspace and Indymedia
- They try to damage the reputation of their victims by posting false information on websites, blogs or user pages
- Many cyber stalkers use third parties to encourage them to join in their pursuit

WHAT IS CYBER STALKING? - III

- Cyber stalkers may attempt to send viruses to their victims computers
- They may order pornographic materials and sex toys, having them sent to their victim's address
- Some cyber stalkers may arrange to meet their victims, especially young people who are at high risk of becoming their victims

DIFFERENT TYPES OF STALKERS

- There are three main types of stalkers:
- Simple obsessional
- Delusional
- Vengeful

SIMPLE OBSESSIONAL STALKERS

- This is the most common type of stalker
- They refuse to believe that the relationship is over despite being told several times
- They have a history of emotionally and verbally abusing and controlling during the relationship
- They may have a history of other criminal behaviors

JOHN HINCKLEY



DELUSIONAL STALKERS

- They have never had any contact with their victims but a false belief that keeps them tied to their victims
- Most of these stalkers suffer from severe mental illness such as Schizophrenia, Bipolar disorder or erotomania
- In erotomania, the stalker believes that the victim loves them even though they have never met the victim
- Rebecca Schaeffer was stalked and killed by Mr. Bardo in 1989 and stalking law came in effect in January 1991 (My Sister Sam show)

REBECCA SCHAEFFER'S HOME



VENGEFUL STALKERS

- These stalkers get very angry at their victims over trivial matters
- They are not motivated by love but vengeance
- They stalk to get 'even' and believe that they have been victimized
- Disgruntled employees, or ex-spouses are common vengeful stalkers
- They are as dangerous as delusional stalkers and are violent
- Mostly males and most of them don't even know their victims (Politicians, organization)

DIFFERENT MOTIVATORS

- Purpose resides in the mind of the stalkers
- Love-Obsession is a common motivating factor among celebrity stalkers
- "Flame war" is normally an argument that is online
- Hate, revenge, vendettas, sexual harassment are common among Predatory stalkers
- They have a desire for contact and control

ONLINE VS OFFLINE STALKING

SIMILARITIES	DIFFERENCES
<ul style="list-style-type: none">• Majority of the stalkers include former intimates• Stranger stalking occurs both in real world and in cyber space• Most stalkers are men and most victims are women• The main motive for stalkers is to control their victim	<ul style="list-style-type: none">• Offline stalking requires both the perpetrator and the victim to be in the same geographical area• Cyber stalkers may be located across the street or in a different country• Cyber stalkers may encourage third parties to harass their victims thru electronic media

TYPOLOGY OF CYBER STALKING

- Primarily, there are three ways of cyber stalking:
- E-mail stalking: Direct communication through e-mail
- Internet stalking: Global communication through internet
- Computer stalking: Unauthorized control of another person's computer

TYPOLOGY OF CYBER STALKING
- E-mail

- One of the most common forms of harassment is unsolicited e-mail which includes obscene, hate or threatening mail.
- Another form of harassment includes sending viruses to the victims or high volumes of junk e-mails or spams in a way to intimidate their victims
- Sometimes cyber stalkers use traditional stalking after sending threatening mails

TYPOLOGY OF CYBER STALKING
- E-mail

- Cyber stalkers can use e-mail to initiate or repair a relationship, or threaten and traumatize a person
- Unsolicited e-mail harassment can jeopardize the privacy of a victim
- It can be argued that e-mail stalking can be less invasive than telephone calls because the victim may undermine the e-mail interaction and delete unsolicited e-mail messages

**TPOLOGY OF CYBER
STALKING - Internet**

- Most Internet cyber stalkers use the internet to slander and endanger their victims
- Proximity takes on a new meaning unlike traditional stalkers
- These cyber stalkers induce emotional distress, fear and apprehension in their victims

**TPOLOGY OF CYBER STALKING
- Computer**

- Computer cyber stalking involves the stalker exploiting the workings of the internet and the Windows operating system in order to assume control over the computer of the targeted victim
- It is a computer-to-computer connection allowing the stalker to take control of the victim's computer
- One needs to be very computer 'savvy' in order to take control of other's computer

**TPOLOGY OF CYBER
STALKING - Computer**

- The only way for a victim to avoid this kind of situation is to completely disconnect the computer and relinquish their current internet address
- Individual computer users have a vastly reduced buffer between themselves and the stalker
- Use of firewalls and wireless routers can resolve some computer hacking problems

ANONYMOUS SERVICES - I

- Another complication is dealing with anonymous communications over the internet
- Cyber stalkers take advantage of the anonymity to avoid accountability for their conduct
- Two different forms of anonymous services are available on the internet

ANONYMOUS SERVICES - II

- The first one allows individuals to create a free electronic mailbox through a website
- Even though they request identifying information, but they never authenticate or confirm this information
- Payment is usually made in advance through the use of money order or other non-traceable forms of payment
- As long as the fee is received in advance by the providers, service is provided to the unknown account holder without any inquiries

ANONYMOUS SERVICES - III

- In the second form, mail servers purposefully strip the identifying information and transport the headers from the electronic mail
- When these mails are forwarded to several of these services serially, a stalker can nearly and perfectly anonymize these messages
- The presence of such services make it easier for cyber stalkers while it becomes a daunting task for others

MENTAL ILLNESS AND CYBER STALKING

- Stalkers can range from cold blooded murders to love sick teens with a variety of mental disorders such as Schizophrenia, and Bipolar disorder
- People with Bipolar Disorder are vulnerable to cyber stalking
- Hyper sexuality often causes damage to relationships, and lead to dangerous behaviors

BIPOLAR DISORDER AND CYBER STALKING

- They have perceptual problems
- Poor impulse control
- Poor self-esteem
- Grandiosity
- Argumentative and irritable behaviors
- Inconsistent and avoidant behaviors

PSYCHOPATHIC STALKERS

Psychopathic Personality Stalker

- Generally male
- Absence of mental disorder
- Targets familiar victims
- Harassment may be anonymous
- Usually some precipitating stressor

Psychotic Personality Stalker

- May be male or female
- Delusions or delusional fixation
- Usually targets strangers
- Attempt to contact the victim
- Absence of precipitating stressor

**FEDERAL CYBER STALKING
LAWS - I**

- It is a federal crime under 18 U.S.C. 875(c) punishable by up to five years in prison and a fine of up to \$250,000, to transmit any communication in interstate or foreign commerce containing a threat to injure the person of another.
- This section 875(c) includes threats transmitted in interstate or foreign commerce via the telephone, e-mail, beepers, or the Internet.

**FEDERAL CYBER STALKING
LAWS - II**

- This section 185 (C) is not an all purpose anti-cyber stalking statute
- It applies only to communications of actual threats
- It is not clear whether it would apply to situations where a cyber stalker harasses or posts messages in bulletin boards or uses chat rooms to encourage others to harass or annoy another person

**LAW ENFORCEMENT RESPONSE -
II**

- Another complication is dealing with anonymous communications over the internet
- Cyber stalkers take advantage of the anonymity to avoid accountability for their conduct
- Two different forms of anonymous services are available on the internet

**FEDERAL CYBER STALKING
LAWS - III**

- Under 47 U.S.C. 223, certain forms of cyber stalking becomes a federal crime, and punishable by up to two years in prison when a person uses telephone or telecommunication devices to harass or annoy others
- 47 U.S.C 22 (a) (1) (c) includes threats and harassment but it is a misdemeanor and punishable by not more than two years in prison

**FEDERAL CYBER STALKING
LAWS - IV**

- The Interstate Stalking Act, was signed into law by President Clinton in 1996, which made it a crime for any person to travel across state lines with the intent to injure or harass another person and, in the course thereof, places that person or a member of that person's family in a reasonable fear of death or serious bodily injury
- Finally, President Clinton signed a bill into law in October 1998 that protects children against online stalking.

**FEDERAL CYBER STALKING
LAWS - V**

- The statute, 18 U.S.C. 2425, makes it a federal crime to use any means of interstate or foreign commerce (such as a telephone line or the Internet) to knowingly communicate with any person with intent to solicit or entice a child into unlawful sexual activity

**CALIFORNIA STATE CYBER
STALKING LAWS - I**

- PC 646.9 covers the Stalking Law in California
- It states that any person who willfully and maliciously, and repeatedly follows or harasses another person and who makes a credible threat with the intent to place that person in reasonable fear for his or her safety or that of an immediate family member is guilty of stalking

**CALIFORNIA STATE CYBER
STALKING LAWS - II**

- The stalking charges can either be a misdemeanor or a felony depending on the aggravating factors and the extent of criminal record of the person
- First time offense without aggravating factors is likely to be a misdemeanor and punishable up to one year county jail time
- Second time stalking offense with the same victim and some aggravating factors would be a felony and punishable up to 5 years in prison

LAW ENFORCEMENT RESPONSE

- Cyber stalking has become a new and challenging crime to be resolved by law enforcement officers
- The first traditional stalking law was enacted by the State of California in 1990
- Since then, law enforcement agencies have developed training and specialized units to deal with cyber stalking crimes
- New York Police Department's Computer investigating and technology unit and LA District Attorney's Stalking and threat assessment unit have majority of these cases

SPECIALIZED TRAINED UNITS I

- Some of the large metropolitan cities such as New York and Los Angeles have developed specialized stalking units
- These units provide specialized training in computer hardware and advanced training which are important in investigating and prosecuting such cyber stalking cases
- The training includes how the chat rooms operate, how to obtain and preserve electronic evidence and how to draft search warrants and subpoenas

SPECIALIZED TRAINED UNITS II

- Other jurisdictions are also taking steps to prevent cyber stalking cases
- One of the critical elements is how to trace communications sent over computers and the internet
- Law enforcement have to be properly trained in computer investigative and legal process, thereby protecting the privacy of legitimate internet users

SPECIALIZED TRAINED UNITS III

- Just like a burglar might leave finger print on the scene of the crime, a cyber stalker may leave 'electronic trail' on the web
- Trained law enforcement may be able to track back to the source and help with the investigative process and eventually help in prosecuting these cases
- Technological proficiency is essential for both the investigators and prosecutors

EFFECTS OF SOCIAL NETWORKING SITES

- With technological advance comes the threat of cyber stalking
- Different social network sites such as Twitter, MySpace, and Face book, are growing rapidly
- Cyber stalkers are taking advantage of these social sites and threatening or harassing their victims online
- People give out information voluntarily not knowing the repercussions until they receive threatening e-mails or hate mails posted

DO'S AND DON'TS OF INTERNET ROMANCE

- Some of the online tips for internet romance:
- Always meet in a public place
- Always tell a friend or a relative about where and when you are going
- Never leave your purse unattended (women)
- Never leave your drink on the table at the bar
- Carry your cell phone with you
- Be aware of your surroundings and remember important landmarks for identification later

GENERAL PUBLIC RECOMMENDATIONS - I

- Any potential cyber stalkers should be reported to authorities when you start receiving hate or threatening e-mails
- Use effective filtering and blocking options on your computer
- Best business practices to be established by addressing illicit activity and /or terminating holders of fraudulent accounts.

**GENERAL PUBLIC
RECOMMENDATIONS - II**

- Do not open unsolicited e-mails or strange/funny looking e-mails
- Be careful by not divulging too much personal information during online chats or e-mails or IM



REFERENCES

- CyberAngels www.cyberangels.org
- Get Net Wise www.getnetwise.org High Technology Crime Investigation Association: <http://www.htcia.org>
- <http://www.usdoj.gov/criminal/cybercrime/cyberstalking.htm>
- Privacy Rights Clearinghouse www.privacyrights.org
- National Center for Victims of Crime www.ncvc.org
- National Domestic Violence Hotline 1-800-799-SAFE (7233); 1-800-787-3224 (TDD)

REFERENCES

- National Sexual Assault Hotline 1-800-656-HOPE (4673)
- SEARCH—The National Consortium for Justice Information & Statistics: <http://www.search.org/>
- U.S. Department of Justice Cybercrime Web Site: <http://www.cybercrime.gov>
- Working to Halt Abuse On Cybercrime Web Site: <http://www.cybercrime.gov> line (WHO@) www.haltabuse.org
