Understanding Cyberstalking through the Analysis of Student's Online Activity

Karen Paullet
paullet@rmu.edu
Robert Morris University
Moon Township, PA 15108

Adnan A. Chawdhry
Chawdhry_a@calu.edu
California University of Pennsylvania
California, PA 15419

Abstract

The Internet has become a medium for people to communicate locally or globally in business, education and their social lives. The increased use of the Internet has created an impact on the number of online harassing/cyberstalking cases. This exploratory study of 121 undergraduate students seeks to examine the extent to which cyberstalking is prevalent. This study argues that cyberstalking and harassment will only decrease when the extent of the problem is fully understood and potential victims and law enforcement understand the protections necessary under the law.

Keywords: Cyberstalking, Online Harassment, Stalking, Electronic Communication

1. INTRODUCTION

Over the years, Internet usage has increased causing an impact on the number of online / harassing cyberstalking cases (Moore, 2018). The primary functions of the Internet are to communicate and research information allowing people to communicate locally or globally in business, education and their social life. The Internet has made it easy for people to compete, meet a companion, or communicate with people on the other side of the world using a mouse click. In 2018, according to the Internet World Stats Report, 320,059,368 people use the Internet in the United States; as a result, there is a concern for Internet safety (Internet World Stats, 2018).

Since the 1990s, stalking and harassing have become more common via the Internet. Until the early 1990's, if a person needed to find information on a given topic for research or a school project, hours could be spent in the library. Some people were lucky enough to have a set of encyclopedias in their homes where a limited amount of information could be found. Public records were always available to people, but one
would have to drive to the local courthouse to locate the records. Going on a family road trip required the purchase of large road maps or trip tickets from the travel agency. In 2018, research, locating records, people, phone numbers, and directions, can occur with the click of a button without one ever having to leave their home. This accessibility to information through using technology has encouraged a relatively new phenomenon called cyberstalking.

The United States Department of Justice defines cyberstalking as the "use of the Internet, e-mail, or other electronic communication devices to stalk another person" (U.S. Attorney General Report, 1999, p.2). Offline stalking is a crime with which many people are familiar. Stalking is a "repetitive pattern of unwanted, harassing or threatening behavior committed by one person against another" (Mechanic, 2000, p. 1). Although offline stalking acts have been reported since the 19th Century, cyberstalking is a crime that is just being examined and reported beginning the late 1990s. The U.S. Attorney General states, "stalking is an existing problem aggravated by a new technology" (U.S. Attorney General Report, 1999, p.2). Similarities have been noted between offline stalking and cyberstalking cases, including the fact that "the majority of cases involve stalking by former intimates, most victims are women, most stalkers are men and stalkers are generally motivated by the desire to control the victim" (U.S. Attorney General Report, 1999, p. 3). Using technology to stalk a victim can include, but is not limited to, the Internet, e-mail, text messaging, global positioning systems (GPS), digital cameras, video cameras, smart phones, blogs and social network sites. One of the differences between cyberstalking and offline stalking is that cyberstalkers face no geographic boundaries. The Internet makes it possible for a person to be stalked virtually anywhere in the world.

This study examines the cyberstalking experiences at the collegiate level. The below research questions will be examined in this study:

RQ1 – What is the relationship between online stalking activities and occurrences of cyberstalking?

RQ2 – What is the level fear associated with victims of cyberstalking?

2. BACKGROUND

The Internet and use of telecommunications technologies have become easily accessible and are used for almost every facet of daily living throughout the world. Cyberstalking is "the use of the Internet, e-mail and other electronic communication devices to stalk another person" (U.S. Attorney General Report, 1999, p.2). For this study, cyberstalking will be referred to as online stalking and is similar to offline stalking, which is being aggravated by new technologies. Cyberstalking "entails the same general characteristics as traditional stalking, but in being transposed into the virtual environment as it is fundamentally transformed" (Ogilvie, 2000). Stalking itself is not a new crime, but cyberstalking is a new way to commit the crime of stalking while using the Internet or other forms of electronic communication devices.

Stalkers, both online and offline, "are motivated by the desire to exert control over their victims and engage in similar types of behavior to accomplish this end" (Ogilvie, 2000) The term cyberstalking can be used interchangeably with online harassment. "A cyberstalker does not present a direct threat to a victim, but follows the victim's online activity to gather information and make threats or other forms of verbal intimidation" (U.S. Attorney General, 1999). A potential stalker may not want to confront and threaten a person offline, but may have no problem threatening or harassing a victim through the Internet or other forms of electronic communications. One can become a target for a cyberstalker through the use of the Internet in many forms. The victim can be contacted by email, instant messaging (IM) programs, via chat rooms, social network sites or the stalker attempting to take over the victim's computer by monitoring what they are doing while online. Bocij, Griffiths and McFarlane (2003) conclude that there are no genuinely reliable statistics that can be used to determine how common cyberstalking incidents occur.

Cyberstalkers can choose someone they know or a complete stranger with the use of a personal computer and the Internet. Basu and Jones (2017) remind us that growing up, our parents told us not to talk to strangers, but one function of the Internet is to talk to strangers. The Internet, as a communication tool, has allowed people the freedom to search for information from anywhere and anyone in the world. Fullerton (2003) states that Internet Service Providers (ISP's) e-mail, web pages, websites, search engines, images, listservs, social media sites are all cyberstalking tools. Other forms of communication used to stalk a victim include cell phones, text messaging, short message services (SMS), global positioning systems (GPS), web cams, or spyware. The information that is available about people on the Internet makes it easy for a cyberstalker to target a victim. With only a few keystrokes, a person can locate information on an individual via the Internet. The types of information that can be found include e-mail addresses, home telephone numbers, bank accounts, credit card information, place of employment and home addresses. Some services, such as Intelius and People Finders, charge to provide confidential information for any person that is willing to pay. Imagine a teacher posting a syllabus online to instruct students what date and time a particular class is in session. Someone that is a cyberstalker can use this small amount of information to follow the instructor to school or try to get inside the instructor's home since they know when they'll be in class. Thanks to searching on the Internet," a cyberstalker can enter a person's home or work address and see where they live or work. Once the cyberstalker can physically see what the home or place of employment looks like, the stalker can use the descriptions of the locations as a way to let the victim know they are being watched.

"The fact that cyberstalking does not involve physical contact may create the misperception that it is more benign than physical stalking" (U.S. Attorney General, 1999). It is not uncommon for cyberstalkers to progress into offline stalkers. "If not stopped early on, some cyberstalkers can become so obsessed with a victim that they escalate their activities to the level of physical stalking (Hitchcock, 2006). Gregorie (2001) indicates that people who do not have access to the Internet, or choose not to go online are not immune from cyber-based crimes. Databases of personal information available on the Internet can enable a person to find the necessary information to stalk or harass a victim.

The anonymous nature of the Internet has left the doors wide open for cybercrimes to be committed. Online stalkers often try to hide their identity by using pseudonyms. Pseudonyms are a way for a person to create a fake name as their identity. The Internet and ISP providers allow people to use pseudonyms. "One can fake gender, age, race and physical appearance" (Fullerton, 2003, p. 2). Offline stalkers are usually within close proximity to their victims, whereas online stalkers can be located virtually anywhere in the world. An online stalker can live next-door, ten blocks away, in another state or even in another country. Just because the stalker may live in another state does not mean that the threats should not be taken seriously. As noted, a cyberstalker's identity can be concealed. The stalkers identity can be blocked from the recipient by using different ISP's or adopting different screen names. More experienced stalkers can use anonymous remailers that make it all but impossible to determine the true identity of the source of an e-mail or electronic communication (U.S. Department of Justice, 2001).

3. METHODOLOGY

The study surveyed students attending two small mid-Atlantic Universities from March to April 2018. The population chosen for this study includes undergraduate and graduate students enrolled in on-campus or online programs. The population was chosen to ensure participants were older than 18 years of age comprising of 121 students. The study collected participant responses using Survey Monkey. The results were imported into SPSS for further organization and analysis. Included in this analysis was to determine correlation using the Chi-square approach with a statistical significance level represented by a .05 margin of error and a 95% margin of error. The study addressed the following two research questions:

RQ1 – What is the relationship between online stalking activities and occurrences of cyberstalking?

RQ2 – What is the level fear associated with victims of cyberstalking?

Prior to administering the survey, the researchers piloted the study with 10 post-graduate students. Their feedback included modifying question wording and updates to the responses listed for each question. The survey consisted of 19 questions, including 1 open-ended question to understand what participants did to end cyberstalking. Additionally, the questions addressed how individuals used the internet, information regarding their cyberstalking, incidents that occurred online and how the participants addressed or notified others when they were involved in an incident.

4. RESULTS

The researchers found it important for the study to examine demographic information related to the participants. Of the participants, 62.81% were female while 37.19% were male. Additionally, 81.82% of the participants were between 18-25 years old with the percentages trailing off as the age categories increased. The results can be seen in Table 1 below. Lastly, students were studied at various levels of education. The distribution consisted of 82.65% of the students being enrolled in undergraduate programs where the largest segment of students at the Junior and Sophomore levels. Lastly, 17.35% of the participants were enrolled in the graduate and post-graduate programs. A further breakdown of participants and their level of education can be found in Table 2 below.

Table 1: Participant Age Distribution

Age	Percent
18 to 25	81.82%
26 to 35	7.44%
36 to 45	5.79%
46 to 55	3.31%
56 to 66	1.65%
Total	100.00%

Table 2: Participants Education Distribution

Education Level	Percent
Freshman	15.70%
Sophomore	28.10%
Junior	23.97%
Senior	14.88%
Masters	15.70%
Doctorate	1.65%
Total	100.00%

One of the survey questions asked if participants have been or currently are a victim of cyberstalking based upon the definition provided at the beginning of the survey. Of the participants, 31.4% stated they had been a victim of cyberstalking. A follow up question was provided to only those who said they were a victim inquiring about how they knew the cyberstalker. Of those who responded they were a victim, 30.56% responded that they did not know the identity of the cyberstalker, while 22.22% stated it was a former boyfriend or girlfriend. Other options included friends, online acquaintance, from school, or from work. The details of these are provided in Table 3 below.

Table 3: Relationship to Cyberstalker

Relationship	Percent
Did not know identity	30.56%
Former boyfriend or girlfriend	22.22%
Friend	5.56%
Online acquaintance	11.11%
School acquaintance	19.44%
Work colleague	0.00%
Other	11.11%
Total	100.00%

Specifically focusing on those who had reported an incident of cyberstalking, the researchers chose to outline any statistical significance that existed between a person's online activities (subject to cyberstalking) and a cyberstalking occurrence. The analysis concluded that any activity producing a chi-square value of less than .05 would have a statistical significance, which included email, web browsing, YouTube, and messaging applications. It is also important to note that social media activities such as Facebook, Twitter, and Snapchat did not have a statistical significance. For a complete listing of the online activities and their associated chi-square values, please see Table 4.

Table 4: Chi-Square Analysis of Online Activities

Online Activity	Chi-Square Value
Email	0.00
Web Browsing	0.00
Online Gaming	0.089
Facebook	0.288
Snapchat	0.23
Instagram	0.315
Twitter	0.265
Youtube	0.04
Skype, Google Hangout, Video conferencing	0.69
Music Applications	0.122
Internet Enabled Mobile Devices	0.304
Messaging Apps	0.039
Blogs	0.41
Dating Sites	0.495

The study examined the length, of these incidents and the level of fear as reported by the participant. Of those who answered they were a victim of a cyberstalking incident, 38.89% stated the incident lasted less than a month. Another 16.67% reported it lasted between 1-3 months. A full breakdown of these lengths can be seen in Table 5. Additionally, 44.44% of the participants who responded they were a victim of a cyberstalking incident stated they feared for their safety during the incident.

Table 5: Length of Incident

Length of Incident	Percentage
Less than one month	38.89%
1-3 months	16.67%
4-6 months	8.33%
7-12 months	11.11%
More than 1 year	11.11%
Ongoing	13.89%
Total	100.00%

The study asked the participants to assess their level of fear related to the incident in terms of low, medium, or high. Of the respondents, 12.5% reported a low level of fear, 50% reported a high level of fear, and 37.5% reported a high-level of fear. Additionally, the researchers found it important to understand how the relationship between the cyberstalker and victim related to their fear for safety. The largest group of respondents who feared for their safety correlated to them not knowing the identity of their cyberstalker while the least was a friend, former boyfriend or girlfriend, or someone they met at school. A breakdown of these relationships versus their fear for the incident can be found in Table 6 below.

Table 6: Cyberstalker Relationship versus Fear

Relationship	No	Yes
Did not know identity	16.67%	13.89%
Former boyfriend or girlfriend	13.89%	8.33%
Friend	5.56%	0.00%
Online acquaintance	2.78%	8.33%
School acquaintance	11.11%	8.33%
Other	5.56%	5.56%

5. DISCUSSION

The participants responded on various activities they did online including social media, communication like text and email, and video conferencing. Interestingly enough, social media sites / tools did not show a statistical significance in this study with the occurrences of cyberstalking. However, other activities like using email, web browsing, youtube, and messaging apps showed a statistical correlation which leads the researchers to believe those activities have attributes making cyberstalking easier. For example, imagine knowing someone's email. You can google it and find out any sites that are linked to it or organization memberships. Or items such as youtube or web browsing allows us to see content we post or like in additional to areas of interest for us. Each of these can provide a single piece of our identifies puzzle but they allow us to continue researching for more information that exists about an individual.

Additionally, it was interesting to see that 30.56% of the participants stated they did not know the identity of their cyberstalker. In prior studies, this metric was approximately 13% which leads to one to believe that an increase in internet activities is directly correlated to the increase in victims not knowing the identity of their cyberstalkers. Over 87% of the participants who stated they were a victim in a cyberstalking incident stated they had a medium or high level of fear for their safety. This is expected given the high value for the participants not knowing the identity of their cyberstalker. However, the fear for safety was reduced when as the relationship was closer to the victim including a former significant other or a friend where our fear was minimal given we know them personally.

Many people wonder what they could have done to avoid or prevent cyberstalking after it happens. Below are some recommendations to minimize the risk of cyberstalking:

1. THINK BEFORE YOU INK. Remember once you send an electronic message it can remain in cyberspace indefinitely.
2. Log off immediately if you experience contact from someone that is hostile, rude or inappropriate.
3. Save all communications from the cyberstalker as evidence.
4. Report the incident to your ISP, law enforcement agency, school administration or an online help agency such as www.haltabuse.org or www.cyberangels.org.
5. Do not post personal information on social media.
6. When online, only type things you would actually say to someone face-to-face. Think about impact of what you say may be interpreted without eye contact, body language or voice.

6. FUTURE RESEARCH

While this study determined relevant issues to cyberstalking at the undergraduate college level, the study did not examine reasons why students that were victimized did not report the incident. Future research should focus on why victims fail to report cyberstalking. Some of the reasons a victim may not report the stalking could include fear, not knowing they could receive help or not knowing whom to report the incident. Additional research is recommended to focus on the financial impact of being a cyberstalking victim. Financial impact could result in a victim changing cell phone numbers or providers, purchasing a new computer or possibly missing work.

7. CONCLUSIONS

Studies are needed to improve our understanding of cyberstalking. The fast pace at which technology changes, as well as, the inexpensive cost of technologies makes it easier for a person to track and stalk a victim. Studies based on victim experiences need to be explored in depth so that the appropriate laws are written to protect victims of cyberstalking. A collaborative effort from victims, law enforcement, and private and public sectors is needed in order to combat cyberstalking and develop an effective response to the problem.

8. REFERENCES

Basu, S., and Jones, R. (22, November 2007). Regulating Cyberstalking. *Journal of Information, Law and Technology*. Retrieved on June 22, 2018 from: http.//go.warwick.ac.uk/jilt/2007_2/basu_jones/

Bocij, P. (2003). Victims of cyberstalking: An exploratory study of harassment perpetrated via the internet. First Monday,Vol 8, No. 10. Retrieved June 29, 2018 from http://www.firstmonday.org/Issues/issue8_10/bocij/index.html

Fullerton, B. (2003, December 22). Features – cyberage stalking. *Law and technology for legal professionals.* Retrieved July 11, 2018 from http://www.llrx.com/node/1114/print

Gregorie, T.M. (2001). Cyberstalking: Dangers on the information superhighway. *National Center for Victims of Crime.* Retrieved May 19, 2018 from http://www.ncvc.org/src/help/cyberstalking.html\

Hitchcock, J.A. (2006). Net crimes and misdemeanors: Outmaneuvering Web Spammers, Stalkers, and Con Artists. Medford, New Jersey: Information Today, Inc.

Internet World Stats (2018, November) Usage and population statistics. Retrieved July 14, 2018 from http://www.internetworldstats.com/stats14.htm

Jaishankar, K. and Sankary, U.V. (2006). Cyberstalking: A global menace in the information super highway. All India Criminology Conference. 16-18 2006 Madurai: India Madurai Kamaraj University.

Mechanic, M. (2000). Fact sheet on stalking. National Violence Against Women Prevention Research Center, University of Missouri at St. Louis. Retrieved April 19, 2018 from http://www.musc.edu/wawprevention.research/stalking/shtml

Moore, A. (2018). Cyberstalking and Women: Facts and Statistics. Retrieved August 30, 2018 from https://www.thoughtco.com/cyberstalking-and-women-facts-3534322

Ogilvie, E. (2000). The internet and cyberstalking. Stalking: Stalking: Criminal Justice Responses Conference, 7-8 December 2000. Sydney: AustralianInstitute of Criminology.

U.S. Department of Justice. (2016). *Stalking and domestic violence:* NCJ 186157, Washington, DC: U.S. Government Printing Office.

U.S. Attorney General Report (1999). Cyberstalking. A new challenge for law enforcement and industry. {Electronic Version} Retrieved July 22, 2018 from http://www.usdoj.gov.criminal/cybercrime/cyberstalking.htm