BEHIND THE SCREENS:
AN ANALYSIS ON CYBERSTALKING

By
TERESA NGUYEN

A Thesis Submitted to The Honors College
In Partial Fulfillment of the Bachelors degree
with Honors in
Management Information Systems
THE UNIVERSITY OF ARIZONA
MAY 2020

Approved by:

Matthew J. Hashim, Ph.D.
Department of Management Information Systems
Table of Contents

Abstract ......................................................................................................................... 2

Introduction .................................................................................................................. 3

Research ......................................................................................................................... 5

   Social Media ............................................................................................................ 5

   Cyberstalkers ......................................................................................................... 7

   Cyber victims ....................................................................................................... 11

Discussion .................................................................................................................... 16

Counter Arguments and Justification ............................................................................ 19

   Civilians .............................................................................................................. 19

   Law Enforcement ................................................................................................. 20

Future Implications of This Study ................................................................................ 21

Future Research Ideas ................................................................................................. 23

Conclusion .................................................................................................................... 24

References ..................................................................................................................... 26
Abstract

Cyberstalking involves the use of social media among other online platforms to gather information and harass an individual. This thesis will explore the inner workings of a typical cyberstalker’s rationale to ascertain whether or not it is possible to determine why they choose to engage in these criminal activities. The research completed will break down the three most common mental disorders among cyberstalkers and assess if there is a correlation between the disorders and one’s inclination to cyberstalk. In addition to this, this thesis will further look into the profile of cyberstalking victims to deduce if it is possible to predict who is more likely at risk of cyberstalking. Similarly, the research conducted will evaluate the impact cyberstalking has on the cyber victims physically and psychologically and how it changes their day to day life. It can be concluded that while there may be similar qualities among cyber victims, it is difficult to pinpoint a defining attribute that would make one more or less likely to be at risk due to the overall ambiguity of the crime. Therefore, while it may not be possible to detect one’s chances of victimization, there are measures that can be taken for individuals to reduce their overall risk, such as being aware of one’s online presence and implementing effective cyber security.
Introduction

Stalking has become a prominent threat in the modern era. More recently, with the rise of social media, a new form of stalking, cyberstalking, has come into play as individuals develop their online presence. Cyberstalking can be defined as “the use of electronic communication to harass or threaten someone with physical harm” (Cyberstalking”, 2020). Cyberstalking differs from stalking itself since it does not necessarily involve any physical boundaries and can be committed from virtually anywhere. However, much like stalking, cyberstalking is a criminal offense under various state laws, including slander and harassment laws. If an individual is convicted of cyberstalking, the punishment for this crime typically includes a restraining order, probation or criminal penalties such as jail. While there may be a fine line between viewing an individual’s Facebook page and cyberstalking them, one’s action can be categorized as cyberstalking if they have inflicted fear on the affected individuals through their actions. If it is evident that the communication between the two individuals is unwanted, then the interaction would fall under the cyberstalking realm.

There are many unintended effects that victims of cyberstalking are forced to endure. For one, they may begin to feel uneasy and struggle to trust those around them. They will also begin to fear that anyone that they come into contact with will be able to cyberstalk them and exploit them thus resulting in their increased reticence towards strangers. Victims of cyberstalking may also suffer from psychological concerns as a result of being cyberstalked, such as depression or anxiety. However, despite the inhibition victims may feel towards strangers, studies have shown that there is an equal chance that their cyberstalker is a previous partner of theirs with each likelihood equal to approximately 30%, respectively (Dreßing, Bailer, Anders, Wagner, &
Gallas, 2014). Virtually anyone has the ability to cyberstalk someone, and virtually anyone who has an online profile can be cyberstalked.

While victims of cyberstalking may choose to seek help, they often struggle to obtain the assistance and resources that they need. In 2017, a Seattle cyberstalking case made headlines when an individual by the name of Francesca Rossi called law enforcement more than twenty times asking them for help regarding her ex-boyfriend, Juan Thompson, who was cyberstalking her (Long, 2018). The response she received, in return, was unhelpful considering her situation. Whenever she reached out for help, she was told to simply turn off her computer. It was not until a separate incident occurred in which Thompson—the perpetrator—made bomb threats against Jewish community centers across the country that law enforcement took action and arrested him. Prior to the bomb threats, Thompson had been harassing his ex-girlfriend online for over a year. During this time, he posted unsolicited pictures of her and sent messages to others in an attempt to damage her reputation. Rossi was always turned away by law enforcement despite seeking help multiple times. To make matters worse, she was unable to take any significant protective measures against him since she did not know his physical address. This curtailed her ability to impose a restraining order against him. An instance of cyberstalking, such as this, caused Rossi to feel incredibly helpless as a result of her inability to escape his constant harassment. Law enforcement was unable to take any actions to stop Thompson. As such, this case shows that despite the harm cyberstalking may cause to an individual’s life, it is difficult to contain it once it has already started.

Although it is hard to stop cyberstalking once it is in action, the purpose of this thesis is to determine whether or not there are any telltale signs of cyberstalking—if any. This analysis will answer the question of whether or not cyberstalking can be predicted either on the
cyberstalker’s end or the victim’s end. While it is evident that cyberstalking may be difficult to control once it has already begun, this thesis is intended to ascertain if cyberstalking can be prevented through early detection. In doing so, I intend to determine if there is any way to effectively prevent or identify a cyber stalker before they implicitly harm the affected individuals. I also intend to determine if there is a way to avoid becoming a victim of a cyberstalking crime as well as if there are any population that is more prone to cyberstalking than others. With this, I plan on conducting a cross-analysis of the records on the psychology of cyberstalkers and the cyberstalking victims to see if there are any defining similarities or differences between the two. Similarly, I plan on researching if there are any concrete means that can be done to prevent such a crime. The resources that will be used in this analysis will be a variety of journals, surveys previously conducted, readings and new stories that have been published regarding this.

Research

Social Media

In this day and age, the role of social media in one’s everyday life is becoming increasingly more prominent. Engaging with various social media platforms is one of the most common activities that individuals partake in as part of their daily routine. Social media allows for users to connect with virtually anyone else in the world whether it is family, friends or even those they have never met before. As such, individuals tend to spend a lot of their free time mindlessly scrolling through social media. For the most part, these subscribers of social media tend to not think twice when they are posting content online. They are able to interact with others by simply making an online profile and provide a few details about themselves. For instance, Facebook is a social media and social networking company with a mission to give people the
power to build a community and bring the world closer together (“Facebook Investor Relations,” n.d). Facebook is the most popular social media platform in the United States as of 2018 according to Forbes (Murnane, 2018). In fact, almost 80% of adults who have access to the Internet and social media in the United States use Facebook (Murnane, 2018). This social media platform provided its users with the ability to virtually befriend and interact with anyone they want from any part of the world.

Facebook, much like other social media platforms, is changing the way the current generation is interacting with one another. While engaging with other users on social media may enhance one’s communication and social skills, studies have shown that those who spend the majority of their time on social media tend to see their real life relationships start to suffer (Amedie, 2015). Individuals are putting the majority of their time and effort into their online presence and how others perceive them online. This, in return, causes them to neglect building and maintaining the existing physical relationships they have with their friends and family offline. Therefore, as those offline relationships begin to deteriorate, they may begin to develop a stronger attachment to those they have come in contact with online despite having never met them (Amedie, 2015). They may post more of their personal information online and be more public about their personal life making it easier for those whom they have never met before to quickly learn about them. Social media has played a crucial role in regards to how individuals choose to portray themselves online since they are now able to manipulate how others see them by posting only what they want others to see (Van Der Velden & El Emam, 2013). This may make one feel the need to “one-up” another individual by posting a picture or a post that they perceive is better than what that particular person posted. This ultimately leads to individuals feeling envious, and at times hatred, towards one another despite the fact that they may not know
the other person and that what the other person posts may not be an accurate depiction of their life or who they are as a person.

The growth and development of communication and information technology has allowed for the upbringing of cyberstalking as a modern issue. As previously mentioned, cyberstalking is oftentimes viewed as an extension of the physical act of stalking. However, it is an easier crime to commit, in a sense, because individuals are able to use these online social media platforms to harass another without having to leave their desk (Wang, Leon, Scott, Chen, Acquisti & Cranor, 2013). These individuals are able to use these online platforms to conceal their identity and commit these crimes, like cyberstalking, without having to come face to face with the impacted individuals. Cyber criminals also have the ability to pose as someone else while committing the acts since they are able to post a picture of anyone online and claim that it is them. Thus making it harder for their true identity to be determined. In addition, social media has made it easier for these criminals to commit this crime since they are also able to simply make multiple accounts after they have been presumably blocked by the victim and continue to contact them. There is no social media platform that is more susceptible to cyberstalking than another.

_Cyberstalkers_

When it comes to those committing the act, it is difficult to find one defining quality that a cyberstalker would exhibit. Based on a survey given to 399 cyber victims, 30.1% stated that their cyberstalkers were generally strangers online who they have never met before while another 29.3% stated that their cyberstalkers were a previous partner of theirs (Dreßing et al., 2014). Acquaintances make up 20.5% of the cyberstalkers according to this survey while friends make up 8% (Dreßing et al., 2014). Among the others listed were fellow classmate, work colleague, previous partner of current partner, family member and distant relative. Therefore, it can be
concluded that cyberstalkers have the potential to be virtually anyone regardless of their known or unknown status with their victims. Cyberstalkers can choose to stalk anyone they come across online (Mitchell, 2010). Their targets can be nonspecific or perhaps even random.

Furthermore, while the relation of the cyberstalkers to their victims tend to be arbitrary, cyberstalkers, themselves, are typically those who are isolated from society, socially awkward, and narcissistic (Spitzberg & Cupach, 2003). They are not aware of their social surroundings and the impact of their actions. At times, they may try to manipulate their victim by coercing or exploiting them. Indeed, those who have never met their victim before may interact with them on social media with the intention of obtaining a relationship with them. Their actions can be threatening and harassing towards the affected individuals, and they may also send the victim unsolicited sexually explicit messages and images. These individuals generally cyberstalk by sending the victim personal messages, sending other people messages with the intention of gathering information or defaming the victim, and spreading lies about the victim especially if they refuse to pursue a relationship with them. Further, if they are not seeking a relationship with their victim, they are likely to be committing the crime to damage the reputation of their target. There is a lot of variance in the methods of cyberstalking and the actions these criminals take.

A study conducted by the *Journal of Family Violence* have shown that a mental disorder, obsessive relational intrusion, is commonly found among those who commit cyber stalking crimes, especially those with the intention of intimacy (Chaulk & Jones, 2011). Obsessive relational intrusion is defined as “repeated and unwanted pursuit and invasion of one's sense of physical or symbolic privacy by another person, either stranger or acquaintance, who desires and/or presumes an intimate relationship” (Cupach & Spitzberg, 2000). Those who may have obsessive relational intrusion tend to pursue relationships with those who are actively against it.
The study identified four types of obsessive relational intrusion behavior: pursuit, violation, threat, and hyper-intimacy with threat and violation as the more threatening forms (Cupach & Spitzberg, 2000). Pursuit is described as trying to make contact with the victim while hyper-intimacy is trying to get the victim’s attention by consistently messaging them and bombarding them with notifications. The threat and violation behavioral categories are both seen as the more serious behaviors related to obsessive relational intrusion since an individual's action would be inflicting harm on their targeted victims. Those with this disorder may exhibit one or all of these behaviors depending on the severity. Mild obsessive relational intrusion behaviors include repeated texts or calls, repeated posts on their social media, and repeatedly contacting them asking for another chance while more severe behaviors include causing hacking into their profile, sending threats to their homes and causing physical harm (Cupach & Spitzberg, 2000). This condition may lead stalkers to maintain a fabricated relationship with another individual in their head. The attraction that they feel towards the other person would thus lead to them consistently contacting them online and cyberstalking them. It is commonly visible in cyberstalking cases to have the main subjects stand in denial of the fact that their previous relationship with that individual no longer exists. Correlation does not necessarily imply causation, but obsessive relational intrusion disorder is a common finding in cyberstalkers. However, this disorder is not a universal or prerequisite factor in declaring someone a cyberstalker; not all cyberstalkers have this disorder.

Further, based on the information provided by the Diagnostic and Statistical Manual of Mental Disorder and the criminal cases conducted by the Los Angeles Police Department’s Threat Management Unit, many cyberstalkers display signs of erotomaniac delusional disorder (Davis, 2001). Those who have this disorder, erotomaniacs, possess the delusional belief that
they are loved by another (MacFarlane & Bocij, 2003). Similar to obsessive relational intrusion, stalkers are willing to go to great lengths in order to get in touch with their targeted victim, which, in return, leads to cyberstalking. Erotomaniacs will believe that their target is in love with them; this disorder may also cause them to create an entire relationship with their targeted victim in their head. Erotomaniacs may overanalyze their targets’ actions online as “signs” that their feelings are being reciprocated even if, in reality, they have had little to no real contact with this individual before. Erotomaniacs may direct obsessive relational intrusion related behaviors towards the affected individuals. However, the key difference between obsessive relational intrusion and erotomaniac delusional disorder is that erotomaniacs believe that another person is in love with them, so they are contacting them because they are already seemingly in an intimate relationship with them in their minds. To them, they are not cyberstalking these individuals but rather contacting someone they are in a relationship with, which in turn normalizes and rationalizes, in their head, the consistent messages and possible explicit images that they are sending.

Sexual addiction and sexual deviance are both crucial factors in the development of cyberstalkers. This addiction is predominantly seen in individuals who are dependent on the Internet whether it is physically or psychologically (Putnam & Maheu, 2000). This condition may have been formed as a result of prior physical, sexual and social trauma (Putnam & Maheu, 2000). Personality disorders, mood disorders as well as substance abuse have all been mentioned as factors that may have contributed to this condition. Those with this disorder may indulge in fulfilling their fantasies through social media and gaming communities (Cooper, Putnam, Planchon & Boies, 1999). They are transfixed to anonymity and sexual deviance, and these online platforms soon become key enablers in cyber crimes. This, in turn, can lead to further
complications since they are convinced that their fantasy world is their reality. They may feel entitled to have a relationship with those they fantasize about online, which becomes a problem if those they fantasize about do not want a relationship with them or do not know about them in general. Relative to cyberstalking specifically, those with online sexual addiction may feel justified to send sexual explicit content to these individuals despite never meeting them before. Therefore, online sexual addiction is another case that, like obsessive relational intrusion and erotomanic delusional disorder, an individual is under the belief that they are in a relationship with someone they are not, which further contributes to cyberstalking.

While those with these disorders and addiction may turn to cyberstalking to get in contact with their victims, not all cyberstalkers have these disorders. Pursuing an intimate relationship is among the main reasons as to why individuals cyberstalk, so these disorders only cover the qualities and motives of those who cyberstalk because they want or have envisioned a relationship with the targeted individual in their mind (Spitzberg & Hoobler, 2002). All in all, cyberstalkers have motives other than an intimate relationship, including defaming the individual, wanting to be the individual or befriending the individual.

Cybervictims

Much like cyberstalkers, there are no definite means of determining how a victim is selected by the cyberstalker. Although some studies have argued that those who are more public about their lives and about themselves on social media are more likely to become a cyber victim, there is still the likelihood that those who are not as active on social media can be victims as well (Mitchell, 2010). As such, among the studies conducted, many have determined that cyberstalking victims are predominantly “more females, more persons with fewer than 12 years of education, more unemployed persons, and fewer singles than in the group of non-victims”
(Dreßing et al., 2014). Of the 399 individuals who have indicated that they have been a victim to cyberstalking, 80.5% of them were female (Dreßing et al., 2014). Females are more likely than males to post personal images and share their personal experiences and stories online. Therefore, women are at greater risk than men in terms of being a cyberstalking victim since a greater percentage of their personal life is made public on social media. Women are also at higher risk since they are more likely to be stalked by a previous partner, such as a former spouse or an ex-boyfriend as mentioned above. In addition to this, demographic data collected from Working to Halt Online Abuse (WHOA) reveals that roughly 30.54% of cyber victims are between 18 and 30 years olds with the large majority of the victims being college students (MacFarlane & Bocij, 2003).

Cyberstalking crimes are more prevalent among college students than in any other population. College students generally do not think twice before they post on social media, and these actions may have repercussions if the wrong individuals get their hands on it. Indeed, when asked, over 40% of the 1,951 college students surveyed stated that they have been stalked before (Reyns, Henson & Fisher, 2011). Another study further supports this by mentioning how out of the 235 university students surveyed, 59% stated that they felt that they had been cyberstalked with 19.6% adding that they felt threatened or in fear of their own safety because of this (MacFarlane & Bocij, 2003). Further studies have also indicated every 14 out of 1,000 individuals over the age of 18 in the United States have fallen victim to cyberstalking (Reyns, Henson & Fisher, 2011). Typically, once individuals reach the age of 18, they are free from their parent’s control and can thus post anything that they would like on social media. Oftentimes, this is also the age that individuals leave for college. Therefore, with the lack of parental guidance
and the newly found freedom of moving away from home for the first time, college students are more likely to be at risk of being cyberstalk.

The lifestyle-routine activities theory hypothesizes that there may be a correlation between an individual's lifestyle and routine and their risk of being a victim of cyberstalking (Holt, & Bossler, 2008). This theory is centralized on the premise that a crime is more likely to occur if there is a motivated offender, suitable target, and no capable guardian meaning no one else present to help the target (Holt, & Bossler, 2008). While not a crucial element for the offender and the target to physically meet in person, it is still pivotal that they cross paths with one another first, in one way or another, in order for the risk to exist. However, those who disagree have countered this by stating that it is presumptuous to assume that criminals are rational during their decision making process (Brunskill, 2014). A cyberstalker does not have to meet or cross paths with their target in order for them to be a potential victim; their chosen target can be an entirely random individual whom they have never interacted with before. In fact, studies have shown that 32.2% of cyber victims have never crossed paths with their cyberstalker before (Sheridan, & Grant, 2007). In addition, while lack of presence of a guardian may make it easier for the cyberstalker to commit the crime, having a guardian present still may not be enough to stop them, especially if said guardian is unaware of what their child does online.

Cyber crime victims will oftentimes change their usual routine as a result of being stalked online. Prevention and protection become a priority. Whether it is taking time off of work or no longer going to events with a large crowd, cyber victims become more wary of what they do in their day-to-day lives. Despite the contact occurring virtually, victims will take protective measures like carrying pepper spray or a weapon on them in case they come in contact with their cyberstalker in person (Short, Linford, Wheatcroft, & Maple, 2014). In addition, they may also
start taking self-defense classes in fear that their cyberstalker may inflict physical harm on them (Short et al., 2014). They will begin to avoid going to any public places, like the grocery store or restaurants, as a precautionary measure. This shows that despite the fact that their cyberstalking is a crime that is committed online, cyber victims will still turn to similar preventive measures as one typically would if they were a victim of stalking. In fact, a little over 16% of the 296 cyberstalking victims surveyed marked that they would avoid seeing their family and friends all together because they did not want to give away their whereabouts in case their cyberstalkers were able to get contact with them (Nobles, Reynolds, Fox & Fisher, 2014). Cyberstalking victims have also changed their personal information as a self protective measure hoping that it would stop their cyberstalker from contacting them with 17.57% stating that they have changed their email address and 14.86% changing their phone number (Nobles et al., 2014). Cyber victims may also install antivirus softwares or a call blocking system in response, but there has been no confirmation that these softwares would decrease one’s risk of cyber-victimization. All in all, over 50% cyber victims have reported taking on one or more forms of self protective behaviors as a result of being cyberstalked (Nobles et al., 2014). Furthermore, studies have shown there is a correlation between the seriousness of the offense and the victim’s decision to seek legal assistance since cyber victims are more likely to seek help if their cyber stalker continuously harasses or threatens them. The duration of the cyberstalking, the threats received — if any, and the likelihood that the victim thinks that the offender will physically attack them all play a role in how serious the victim perceives the cyberstalking offense.

Those who are victims of cyberstalking experience a variety of psychosomatic and psychosocial problems even after the incident has been resolved. Of the 399 cyber victims surveyed by *Cyberpsychology, Behavior, and Social Networking*, 78.2% reported feelings of
inner unrest with 68.2% reporting that they began to feel uneasy and wary of other people (Dreßing et al., 2014). As a result of being cyberstalked, victims now have difficulty trusting those around them because they do not know who knows who and are conflicted on who they can truly trust now. They may also start to feel reticence towards strangers because of this as well. They do not know who has malicious intentions and who does not. Therefore, their subconscious thoughts ultimately cause them to mistrust a large majority of those around them. They are also often afraid to go into new relationships because of this. They are fearful that whoever they choose to date may either end up cyberstalking them if they were to end; cyber victims also fear that any potential relationship with someone can be a connection that their cyberstalker is using to get to them, among other reasons. However, on the other hand, if they are able to trust another individual enough to pursue a relationship with them, 22.3% have still reported to have partnership issues (Dreßing et al., 2014). Cyber victims have their guards up, even after their cyberstalker has stopped their pursuit, but despite that, cyber victims will continue to have difficulty fully trusting someone and allowing them to be a part of their life. Furthermore, two thirds of these individuals noted that they have sleep disturbances and over half reported feelings of helplessness and anger as a result of being a victim to this crime (Dreßing et al., 2014). Especially in the cases where the victim does not know who their cyberstalker is, they will constantly be worried since they do not know what information their cyberstalker has about them and to what extent they would go to to get their attention or hurt them. Cyber victims feel helpless at times discerning that they may have lost control because they do not know what they can do to lose contact with the person who is cyberstalking them. Many of these individuals may also develop more serious conditions like depression because of their experience (Tennant, Demaray, Coyle & Malecki, 2015). Along with no longer feeling the need or desire to socialize
with others, they may have trouble concentrating on what used to be important to them. All in all, the lives of cyber victims changes drastically during and even after they have been cyberstalked.

**Discussion**

In terms of prevention, cyberstalking may be difficult to prevent from happening. Even though there has been many studies done on cyberstalkers, it is difficult to pinpoint the exact qualities that cyberstalkers have since many of them do not share any similar qualities. It may also be untimely to assume that those with a certain mental illness, like obsessive relational intrusion, will be cyberstalkers since individuals who have this disorder may not make attempts to virtually contact that person. Furthermore, although the mental disorders listed above may indicate those who are more prone to cyberstalk, not all cyberstalkers are mentally ill. Some individuals may cyberstalk simply to get attention whether it is for themselves or from their targets (Reichart Smith, Smith, & Blazka, 2017).

In regard to early detection or prevention, it is difficult to detect these mental disorders since many of these individuals do not have the resources to go and be diagnosed, or worse, they do not believe that there is anything wrong with them, so they have no desire to seek help. However, if these mental disorders were able to be identified, then, cyberstalkers may be able to be identified. These disorders can be detectable if the individual speaks to a third party, such as a professional consultant. On their own, they may not believe that they are doing anything wrong, but if discussed with others, they may be able acknowledge the fault in their ways.

As said before, in many of the current cyberstalking cases, the cyberstalker was a previous partner of the cyber victim. Due to the nature of the relationship between the cyber victim and cyberstalker, each case can be circumstantial. For instance, at the end of a
relationship, especially, with those who do not want the relationship to end, those individuals may resort to extreme measures, such as cyberstalking. They would consistently contact their previous partner online in hopes that they would be able to reignite the flame and salvage their relationship or simply in vengeance for the pain that that person may have caused them. On the victim’s end, it may be difficult for them to file a restraining order against their cyberstalker and ex-partner, for example, since they may not know their new permanent address. This is applicable to many cyberstalking cases since social media allows for one to stalk another remotely thus making it harder to file a restraining order against them since there is no way for them to distinguish exactly where they are located.

Much like the cases for cyberstalkers, it is also difficult to determine which individuals may be at risk of being a victim of cyberstalking. Although studies have shown that the ages of cyber victims centralize between the ranges of 18 to 30 years old, those outside of this range are at equal risk. However, when surveying college students, specifically, over 40% of them stated that they have been cyberstalked before (Reyns, Henson & Fisher, 2011). While on the lower end of the typical age range, it is not surprising that many college students have been victims of cyberstalking before since college students are more likely than other demographics to publicize their personal life online. As a result, this increases the likelihood that they become victims of cyberstalking. By providing their personal information online, they may be seemingly making it easier for cyberstalkers to gather information on them and possibly use it against them. Further, cyberstalking can be detrimental to college students in the long run since at the end of the day, they are still very young and impressionable. They are developing their adult habits at this age with many students being away from home for the first time. They may be in a complete new environment with no one to turn to. Consequently, cyberstalking may cause anxiety among
college students that they will carry along with them as they progress through the rest of their adult lives.

Individuals may be able to reduce the likelihood that they become cyber victims by changing their digital lifestyles and being self-aware of their online presence. Internet users and social media users must realize the availability of the information that they post publicly online. Even if their privacy settings are set to “Friends Only,” those outside of their immediate circle may still be able to access their information. Through proper awareness training and exposure to security programs such as McAfee, for instance, individuals may be more likely to reduce—but not fully eliminate—their risk of vulnerability to cyber crimes. The simple act of not posting locations, geotags, birthdays, photos, or other personally identifying information can drastically reduce their ability of getting cyberstalked. The presence of social media in one’s daily lives provides ample information to cyberstalkers, but it would be much more difficult for a cyberstalker to find valuable information about potential victims if individuals limit the information that they share online. In addition to that, individuals should also be aware that what they like, share, or re-tweet online divulge much more information about themselves than they would generally expect. All of this information, from geotags to likes, is what cyberstalkers would use to take advantage of people and thus violate their privacy.

All in all, the best way to combat cyberstalking is by reducing one’s social media footprint and buying effective cybersecurity measures. Entrusting a company with one’s privacy and security might sound somewhat concerning and counterintuitive at first since doing so would be voluntarily giving one’s personal information to a third party. However, it is important to acknowledge that in order for one’s information to be secure, one must secure the device that holds all the information first. Furthermore, once the vast majority of the world realizes that
there is minimal legislation in place to manage, prevent, and adjudicate cyber activity—let alone cyber crimes—, they may be more likely to take their own preventive measures to protect their personal information and devices. Cyber criminals will always be on the hunt for their next target, but the best way to keep them out of one’s life is to reduce the personally identifying information that we provide them and stop them in their tracks with the right security programs and firewalls.

**Counter Arguments and Justification**

*Civilians*

As stated previously in this document, cyberstalking is a criminal offense that falls under a handful of state laws. However, there is a fine line between cyberstalking and simply researching public information on someone. Therefore, the difference between cyberstalking and doing research on someone needs to be clarified. The majority of activities that involve looking up an individual online are typically in a negative context, but there are some cases where researching public information on individuals can be used to aid people in protecting themselves. In a sense, researching information on an individual may be classified along the same lines as cyberstalking, but it is not due to the fact that there is no malicious intent behind the act. For that reason, looking up information on an individual online can be justified if the information is gathered solely for protective measures and there is no intent on using the information found to harm that person.

While it could loosely be categorized as cyberstalking, a civilian who has the need to check public records of someone online can do so as long as it is not with criminal intentions or is intended to incite fear. For example, it is a common practice to scan social media platforms to gather known information for blind dates, background checks, and so forth. This action would
not be classified as the same cyberstalking that cybercriminals conduct since the information collected is not meant to be used in a harmful manner. Instead, this would be considered as simply researching public information on an individual of interest oftentimes for protective measures like assuring that one’s blind date is not a potential risk to meet, for instance. This action of what could be considered good-natured research can, therefore, be justified so long as there is no intent to exploit such information against that individual’s will or use that information for further harassment or for unethical reasons. Consequently, although this action may seem to fall under the variation of “cyberstalking,” as some might call it, it is not criminal due to the lack of harmful intent behind it.

*Law Enforcement*

Another justification for cyberstalking is in line with how various law enforcement entities utilizes it. While again, “cyberstalking” is a subjective term for both law enforcement and conventional civilians, it is important to be able to differentiate when it is used as a tool for combating criminals and when it is used to commit a crime (Brunty & Helenek, 2014). Law enforcement agencies abroad have been using information made publicly available in the aid of tracking, deceiving, and incarcerating a broad selection of criminals. In this sense, “cyberstalking”, when it is used in the context of police researching individuals, and “cyber-harassing”, when it is used by police in the effort of entrapping predators, for example, are both justified by their means. Both of these actions, when used by law enforcement, is being used for the greater good of catching those who are committing serious crimes?

As noted in *Data and Civil Rights*, when the police use false social media accounts in a research effort to gather evidence of criminal activity, for example, the action of cyberstalking is acceptable (Mateescu, Brunton, Rosenblat, Patton, Gold & Boyd, 2015). For instance, as the
article quotes in a previous interview, many criminals have posted damning evidence of their crimes on social media essentially exposing themselves by providing the media proof of their guilt (Mateescu et al., 2015). Their affiliations, actions, status, location, behavior, and other intelligence matters then become public knowledge as a result of their post. Therefore, law enforcement would be justified in having a misleading social media account to attain this information. Even at that, when the information that the police seek is not in a criminal manner and is simply used to just “fill in the blanks” of what they need to know as opposed to tracking and monitoring their criminal activities, they would be able to use open source search platforms to scan for other identifying information. This is similar to civilians looking up information of others online, except with law enforcement, they are doing so generally to assist in their capture of a criminal. Law enforcement also do not necessarily need a warrant to do this type of online search depending on the circumstances since much of the information they use is public information that is available online. Thus, law enforcement authorities are able to use this information in the further prosecution of detainees, apprehension of predators, and overall prevention of criminal activity. This, in it of itself, is cyberstalking, but is justified by its intentions by police.

Future Implications of Thesis

The takeaways of this thesis reveal the current status of cyberstalking crimes and their relevance in the modern world. In addition to this, this thesis identifies the common persona of the typical cyberstalkers and the selected cyberstalking victims. After reviewing the reported psychological impact that cyberstalking has on its victims as well as the statistics gathered, it is especially evident that further laws, preventive measures and awareness needs to be spread. There needs to be more expansive legal measures in place in order to help prosecute criminals,
who operate on this new frontier of cyber crime. Cyberstalkers operate in the gray area of the law and often evade capture due to their ambiguous nature, civil liberties and lack of laws regarding the crime. However, in this constant tug-of-war between privacy, encroachment and justice, it has become nearly impossible for the legal system to properly eradicate these types of crimes due to the continued advancement in technology that cyberstalkers can use to their advantage. As such, the only effective measure of handling these pending threats towards society is through prevention. By introducing the public to preventive measures, such as firewalls, enhanced authentication measures, private profiles and other means of physical and cyber security, the risk of being cyberstalked would be reduced. Therefore, these preventive measures are the only logical ways to curtail the furtherance of cyberstalking.

It can be assumed that, by this point, only big business and corporate entities will be able to afford and provide effective security for customers, victims and others. The government currently does not have the means to be able to combat these types of crimes without jeopardizing the civil liberties of civilians, whether they are victims or criminals. Thus, the privatization of internet security and cybersecurity options is likely to be the future solution for combating cyber crimes. This, unfortunately, does imply that only the select few that can afford these advanced cyber security platforms will be the ones who will be relatively protected from cyberstalking and security breaches. Malicious spyware, sturdy firewalls, and uncontrollable internet behavior all work against each other to create the present situation. Cyberstalking is an unforeseeable crime and a developing whirlwind that changes its form, capabilities and direction over time especially as technology advances. There is likely to be a constant threat against internet users of the future, and it will become the responsibility of the common individual to be able to effectively protect themselves against their own vulnerabilities towards cyberstalking.
Future Research Ideas

Based on the findings of this thesis, a survey would help to better understand the impact cyberstalking has on its victims. However, due to the recent pandemic, we were unable to conduct a survey regarding our analysis. Therefore, some potential survey questions, specifically addressed to cyber victims, that can be ask in the furtherance of the aforementioned research may include:

• What was your relationship to your cyberstalker?

• What cyberstalking behavior did you experience?
  
  o Did your cyberstalker send you threatening messages, try to damage your reputation, etc.?

• Which social media platforms are you on—if any?

• Did you tell anyone (i.e. parent, guardian, friend, law enforcement) about your cyberstalking experience while it was happening?
  
  o If so, how long did you wait until you reached out to someone?
  
  o Looking back, do you think there was anything that could have been done to help your situation?

• Did you fear for your safety?

• What impact did cyberstalking have on you?

• Did you take any preventive measures to protect yourself as a result of cyberstalking?

These questions are directed towards cyber victims due to the assumption that cyberstalkers would be more difficult to identify and get in contact with. Based on the age groups found in the research, college students would be the ideal candidates to test. The survey can be sent out to them on an online format in an email, and they would be able to answer the questions
Anonymously. Further, the collection of these survey results would help one better comprehend the overall influence of cyberstalking on a victim’s day to day life.

Conclusion

This thesis revealed that there are minimal to no telltale signs of cyberstalkers or cyberstalking victims. As such, it is evident that there is an uncontrollable and even undetectable nature of cyber crimes. Cyberstalking is a covert, destructive and untraceable act of harassment against individuals. There is no feasible way to track the profile of a cyberstalker whether it is through search functions, downloads of computer programs or internet history since cyberstalkers may be cunning enough to cover their tracks by using a private browser or a public computer. Depending on each scenario, there is also not a definite way to cross-reference the profile of a cyberstalker to an individual. Some cyberstalkers may have multiple profiles while others may have a profile under a pseudonym in order to conceal their true identity. Either way, the ability cyberstalkers have to mask their identity makes it more complex to stop them. In addition, the studies referenced above have revealed that there is no outstanding way to prevent the progression of these crimes or determine the probability of victimization. Therefore, for as long as there is cyberspace, cyber crime will continue to persist in this world, unfortunately, thus implying that cyberstalking will always be around. Those who can manage to protect themselves and their presence online will likely surpass the longevity of those who cannot. The further implications of this thesis include the notion that sooner or later, all individuals will seek cybersecurity packages from big businesses in order to protect themselves. There will not be any substantial legislation any time soon that thwarts the furtherance of these crimes. The government has laid out the path for private entities to dominate in this market and serve as the face of counteracting cyber crimes. Therefore, individuals must take it upon themselves to
reduce their risk of becoming cyber victims by being aware of their online presence and obtain
the necessary softwares to protect their data.
References


