Cyberstalking/Cyber-Harassment:

Understanding this Type of Criminal to Aid in Convictions

Rachael Riggs

National American University

Henley-Putnam School of Strategic Security

SEC665: CYBERSECURITY

Dr. Ray Curts

March 2023

Abstract

This paper focuses on the issue of cyberstalking and the importance of implementing a way to prosecute and convict stalking offenders adequately. Cyberstalking is one of the fastest-growing crimes, yet it still is largely unreported and undertrained in police departments. Victims often do not feel safe reporting the crime or feel that they will not witness a positive outcome or that the police will do nothing. This idea needs to change, and we examine what needs to occur to change this viewpoint.

Also discussed are issues with law enforcement and how they can better investigate and prosecute the Cyberstalker. Ways to train the officers, a collaboration between officers and victims, and new software for police departments will be the focus of this paper.

Table of Contents

Cyberstalking/Cyber-Harassment:

Understanding this Type of Criminal to Aid in Convictions

Stalking is any form of repeated contact that causes an individual to feel afraid, harassed, helpless, or like they have lost their sense of safety and security. This contact may occur in person or online. 7.5 million people are affected annually, with women being far more likely victims than men. (Fitzpatrick, 2023)

Introduction

Less than 1/3 of stalking victims report the crime, and 67% of stalking victims fear physical harm or death. The approximate numbers show that only 0.3% of reported cybercrime complaints are enforced and prosecuted. (Hechler, 2021) (MacKenzie, et al., 2011)

The Question

What can be done within the next three years to help victims and law enforcement work together to increase reporting and prosecution of cyberstalking criminals in the United States?

Discussing the Issue

"CYBERSTALKING IS ONLINE HARASSMENT, BY EMAIL, CHAT, INSTANT MESSAGING OR OTHER MEANS, THAT SERVES NO USEFUL PURPOSE OTHER THAN TO CAUSE EMOTIONAL DISTRESS TO THE VICTIM WHILE LAYING THE GROUNDWORK FOR DANGER LATER ON. THE STALKER MAY DO SO TO INTIMIDATE, OFTEN BEFORE KIDNAPPING, HOMICIDE, OR SEXUAL BATTERY. " (Pueblo County Sheriffs Office, 2023)

Cyberstalking or Cyber-harassment, occurring from a partner or otherwise, is a growing concern and happens much more often than statistically shown. Cyberstalking can take place in the form of fake social media profiles, mean comments, humiliation, trickery, trolling, catfishing, or online harassment, to name a few. (Sevens Legal APC, n.d.)

Often a victim does not contact the police because of reasons of knowing the victim, not thinking what is happening is illegal, not understanding what is happening, or the victim does not even realize the crime is taking place. Victims of this type of crime and law enforcement should understand the potential for severe harm or death to the victim by the offender. In addition, many victims of cyberstalking or cyber-harassment will face psychological problems, including depression, anxiety, PTSD, hypervigilance, and lower self-esteem, to name a few. (MacKenzie, et al., 2011)

If law enforcement does have information on this underreported crime, there is often little they can do about it. One of the issues faced is that of jurisdiction. (Grimes, 2016) When it takes place online, it could be intrastate or even dealing with situations in other countries. The first traditional stalking laws were not enacted until 1990, making stalking new to law enforcement.

Regarding cyberstalking, police are still trying to navigate the challenges and prepare the officers with the proper training and expertise. (A Report from the Attorney General to the Vice President, 1999) (Brown C. S., 2015) Furthermore, It can be hard to charge when it is hard to prove. When a person creates a fake account and sends an email or posts on social media with a fake profile, if the individual claims they did not commit the act, the investigators must prove that this person committed the crime. Finally, there is the issue that the offender may claim he has freedom of speech. (Hechler, 2021) (Wright, 2020)

Understanding the type of personality that utilizes technology to commit these crimes is essential. This understanding will better aid law enforcement during investigations and help victims become more aware of their situation. Also necessary to the research of Cyberstalking/Cyber-harassment is understanding actions taken and the crimes committed against the victims; this will better inform victims and law enforcement in identifying abuse and helping to minimize it while maximizing evidence against the offender. Also, we will consider ways that law enforcement can gain an advantage in acquiring necessary evidence. Lastly, we will examine how the prosecution works with this crime, how to address underreporting, and if our current way of handling these cases is effective.

Research Questions

1. Personality Profile of a Cyberstalker
2. Victim profile and understand the crimes of a Cyber-stalker against his victim.
3. Crimes committed against the victim
4. How can the victim better protect themselves?
5. How can law enforcement or a victim gain an advantage in gathering and maintaining evidence of the acts?
6. How is Cyberstalking charged and prosecuted?
7. The way we currently handle cyberstalking, is it effective?

Chapter 4: Literature Review

The literature used as sources within this research paper help provide background information on the issue and explain the laws associated with cyberstalking and cyber-harassment. Though we have made substantial progress since the first stalking laws of 1990, the 1999 report from the attorney general to the vice president (A Report from the Attorney General to the Vice President, 1999) lists all of the issues that we still face today though probably on a much lesser scale.

The article from the Cyber Crime Journal (Brown C. S., 2015) lists many of the issues faced today by law enforcement. It also discusses the role of the victim and the importance of reporting. The CSO Online article (Grimes, 2016), the Dispatch article (Dispatch et al., 2012), and Cyber Security News (Hechler, 2021) all explore the reasons why it is hard prosecuting cyber criminals and crimes of this nature.

Doctors and professors jointly contributed to the quality content on the site titled "Stalking Risk Profile." (MacKenzie et al., 2011) The quote and information provided by the Pueblo County sheriff (Pueblo County Sheriff's Office, 2023) come from a reliable source and provides views others have yet to explore. The article Sevens Legal (Sevens et al.) discusses what cyberbullying is and when it has turned into a crime.

The UNODC article (UNODC, 2020) discusses global issues and how to recognize cyberstalking when it occurs. Whitemore's article written for the Department of Sociology (Whitemire, 2020) discusses almost every issue one will face concerning cyberstalking, including modes of doing, issues or concerns, tactics, the victim-offender relationship, variables, outcomes, control variables, analysis, and unique cases to name a few—things provided in this

paper. Finally, Wright (Wright, 2020) discusses the issues with cyber-harassment and how it applies to freedom of speech.

The US Department of Justice's stalking victimization Statistics up to 2019 (Morgan & Truman, 2022) provide valuable statistics on all stalking in the United States up to 2019. The reference for WHOA (Working to Halt Online Abuse) provides statistical data up to 2013. (WHOA, 2013) Kaspersky is a well-known antivirus software that provides information on its website for ways to protect oneself against all cybercrime. (Kaspersky, 2023)

Michael Nuccitelli is a physician and an expert in the area of stalking and has dedicated much of his time to bringing awareness to cyberstalking with many excellent sites to reference and valuable information contained. (Nuccitelli M. P., 2023) (Nuccitelli M. P.)

In gaining information on the psychology or pathology of a stalker, it is necessary to utilize references from reputable authors that have done their research. This information came from Sandra Brown's article as well as the "Distinct Pathological Profiles of Inmates." (Brown S. L., 2012) (Dellazizzo et al., 2018)

The FBI is highly relevant regarding cyberstalking, cases, information to protect oneself, and a webpage for reporting this crime. (FBI, 2023)

Summary

The research here came into existence because of the realization that there was a need to find ways to help cyberstalking victims come forward and report the crimes against them; this, in turn, would allow law enforcement to establish better ways to prosecute and adhere to stricter punishments on those that commit such crimes against others.

As stated in the introduction and deserves repeating, “less than 1/3 of stalking victims report the crime, and 67% of stalking victims fear physical harm or death. Only 0.3% of all reported cybercrime complaints are enforced and prosecuted.”

Stalking has become incredibly easy since the perpetrator can remain hidden behind a screen while monitoring the victim's every move and plotting against her. This type of stalker is just as frightening as the one that follows you home from work. What the Cyberstalker has over the traditional stalker is all of the victim's communications available at his fingertip and potentially knowing their private thoughts as he reads your online diaries, letters, and emails. The Cyberstalker can get inside the head of his stalker and use her weaknesses against her, all while keeping tabs on her every move and private communication, which would be much more difficult for the traditional stalker.

From the victim's perspective, there are several reasons they may not report that they are a victim of cyberstalking. A few of those reasons seen are:

- They may not know that what the person is doing is a crime.
- They think law enforcement cannot or will not help them.
- They might know the victim and do not want to report this person.
- They may be scared to report. (Possibly having been threatened)

These are all issues that dealing with should be a priority. There are ways to counter them by allowing the necessary information to get to the public and giving the victims of the crime the knowledge to make a choice, as well as the security of knowing that their choice will not leave them out in the cold to fend for themselves. (this aspect being the harder of the two to accomplish confidently).

The research of this paper is to help fill this void in law enforcement and the separation they have from the victims of this crime. Cyberstalking is on the rise, and more and more people are affected daily. A person that experiences cyberstalking and harassment has long-term mental health issues, including issues of depression, anxiety, and PTSD. Finding ways to prosecute those that create these unsafe environments for others is crucial. Without this, the number of victims will continue to rise, and the number of convictions will stay stagnant. With the information from this research, the hope is that the opposite will happen with the numbers, and the victims will feel confident in reporting knowing that their safety is a top concern.

As this shift begins and people begin to realize that there is help for crimes against them in the cyber world, the hope is that citizens will begin to feel a higher sense of peace and gain trust in their law enforcement to protect them in the cyber domain just as they have already established their trust in situations such as during a home intrusion.

One thing seen from the research that has worked is awareness campaigns such as those that have swept the nation in response to cyberbullying, which is very similar in circumstances to the harassment in cyberstalking. The first step is bringing awareness and understanding of cyberstalking to the public.

Once awareness has been established, it is vital to ensure that the victims know that what is happening is a crime and that they can escape the situation *safely*.

To best accomplish getting the information out to the public is through awareness campaigns, marketing campaigns, bulk advertisement, targeted ads, social media campaigns, press releases, speaking engagements, lectures, print, media interviews, brochures in the workplace and schools, and other ideas for consideration throughout the campaign.

As the experiment has yet to implement, this research serves as the initial starting point in deciding what needs to occur, why, and the best ways to begin the transition. To begin the initial research, we must answer the questions in the paper.

Question 1: Personality Profile of a Cyberstalker

As is the case with traditional stalking, so too is it with cyberstalking that most perpetrators are men. 80% of women and 65% of men know the identity of their stalker. Information on stalkers and their profiles suggests there are five types of stalkers. (Nuccitelli M. P.)

1. Rejected Stalkers- these individuals are angry at a perceived wrong and seek revenge.
2. Resentful Stalkers-Believes the victim deserves fear and distress. The stalker is fulfilling a vendetta against the victim for some anguish they have caused them.
3. Intimacy Seekers- Seeks a loving relationship with another they view as their soulmate. (Typical of the celebrity stalker)

4. Incompetent Suitors- This stalker lacks social, communication, and courting skills. They feel entitled to a relationship with the victim and will slowly increase their contact.
5. Predatory Stalkers-This is a very dangerous and determined stalker motivated by sexual desires. They desire to control and victimize, and their personalities are similar to that of a sociopath. (Nuccitelli M. P.)

Cyber-stalkers are motivated by a multitude of factors, including:

- Psychiatric illness
- Obsessions
- Revenge/hate
- Jealousy
- Control
- Sexual desire

(Nuccitelli M. P.)

Low empathy is a core trait of a pathological disorder that leads to inevitable harm to another. (Brown S. L., 2012) Without empathy, individuals have reduced conscience, remorse, and guilt and may even enjoy seeing pain, discomfort, or harming others. Cyberstalkers of every type (aside from that of the intimacy seeker, which often correlates with an individual having learning or developmental disorders. (Nuccitelli M. P.)) often share common traits. Those traits are "symptoms related to impulse control, reduced empathy and conscience, emotional regulation disorders, a lack of fear of consequences, pleasure in harming others, and a reduced learning from negative experiences." (Brown S. L., 2012) These personality traits belong to a group of personality disorders known as cluster B.

Cluster B personality types include Histrionic Personality Disordered, Borderline Personality Disorder, Narcissistic Personality Disorder, Anti-Social Personality Disorder, and sociopathic and psychopathic personality disorder. (Brown S. L., 2012)

Cluster B personality behaviors stem from a "complex interweaving of emotional, developmental, neuro, biochemical, and even genetic abnormalities." (Brown et al., 2012) This personality cluster brings the most damage and makes up most of the prison population. Within this group, clusters 3 and 4, Cluster 3, "*Early-onset violent delinquents*," emerged as more severely anti-social. Cluster 4, "*Early-onset unstable-mentally ill delinquents*, exhibited the most server psychopathological and criminal characteristics. (Dellazizzo, et al., 2018)

The combination of addictive disorders and personality disorders escalates criminal behavior and has the highest rates of criminal conduct that will lead to an offender in jail. (Flórez, et al., 2019) Most of the prison population harbors one or the other and often both. This information is highly relevant to that of a cyberstalker.

Question 2: Victim Profile

Women are more often the victim than men, with a ratio of 3-1. However, the rates of child victims are rising with the stalker being an adult. (Nuccitelli M. P.) The majority of victims are between the ages of 18-40. A 2013 WHOA statistical analysis states that 78% of victims are Caucasian, 52% are single, 53% had a prior relationship with the harasser, and the majority of 47% is an ex. (WHOA, 2013)

25% of victims had threats of offline violence from their harassers. 75% of the victims reported harassment. (WHOA, 2013)

- ISP 35%
- Police 37%
- Lawyer 14%
- Web site 14%

> Of these cases, Only 25% were referred to law enforcement, and WHOA handled 68%. WHOA handled these situations by contacting the ISP, web admin/host, or advising the victim to change usernames, email addresses, profiles, options, or preferences. (WHOA, 2013)

The data from the 2019 stalking victimization statistics show that *67% of cyberstalking was never reported to the police.* The biggest reasons for not reporting are that *victims felt it was unimportant, dealt with it another way, or felt that police could not or would not help.* (Morgan & Truman, 2022)

This data shows that cyberstalking victims likely feel nothing can be done to help them, and their faith in police ability may have diminished.

Only 29% of the cases involved victims and harassers in the same state/country, which is one of the issues concerning law enforcement and jurisdiction. The top location for both victim and offender is California, Florida, and Texas. (WHOA, 2013)

Question 3: Crimes committed against the victim.

The same WHOA 2013 statistical analysis showed that harassment began with email at 30% and Facebook at 30%, with the exact prevalence. Next up is a Web site at 14% and IM at 42%, with texting at only 8% and dating sites at 3%.

Escalation took place in the following way:

Facebook *29%*, Phone *25%,* Text Message *24%,* Twitter *17%,* Google+ *17%,* Email *16%,* Dating Site *15%,* Web Site *15%,* Forged profiles *12%,* Face to Face *9%,* Postal *8%,* Msg Board *8%,* Myspac*e 4%*, Blogs *3%,* YouTube *3 %,* Vimeo *3%,* Craigslist *2%.*

Common ways a cyberstalker will harass his victim:

- Electronic messaging such as classic emails, text messages, and Twitter.
- **II.** Spamming or sending threatening emails to the victim or the victim's family, friends, or co-workers.
- **III.** Posting the victim's personal information such as name, address, phone number, and email address online.
- **IV.** Posting offensive comments in the victim's name.
- **V.** Creating and posting sexually explicit images of the victim or the victim's loved ones.
- **VI.** Hacking into the victim's computer, accounts, and mobile devices.
- **VII.** Subscribing the victim to pornography sites and unwanted advertising.
- **VIII.** Attaching spyware to emails or installing it on the computer.
- **IX.** Setting up websites that threaten the victim or encourage others to contact, harass or harm them.
- **X.** Computer Monitoring Software, or "Spyware," allows a cyberstalker to monitor computer and Internet activities and discover a victim's efforts to escape or access help. This software can be installed remotely or by physically accessing the victim's computer (Nuccitelli M. P., 2023)

Question 4: How can a victim better protect themselves?

To protect themselves online, every person should educate themselves on cyberstalking and the signs of it as well as the type of person, keep what they disclose about themselves to a minimum, set boundaries regarding personal information and the sharing of such, do not

socialize with those you do not know, know the laws in your area concerning cyber harassment. (Nuccitelli M. P.)

Enhancing privacy settings is one of the first things a victim should do. Be sure to shut off locations and location tracking. It may be necessary to go into each app and turn off the location tracking of the app. Using a false name on social media accounts to prevent the offender from finding the victim profile, labeling as gender-neutral, removing oneself from "Locator" or "finder" websites such as "TruthFinder," "BeenVerified," and "Intelius." (This requires going to each website and requesting to be removed, time-consuming but essential.) Limit the audience of your posts and pictures on social media. Do not add any person to your friends list you do not know personally, and do not communicate in private messages with anyone unknown. (Kaspersky, 2023)

Secure your PC and Phone with a strong antivirus and malware software and use a VPN. Do not use public wifi, keep a lock on your phone and keep it on you at all times, never leaving it where someone else may access it without you knowing. Use anti-spyware, always log out of your accounts, and Use a strong lock on your computer and your online accounts (Kaspersky, 2023), being sure to utilize two-factor authentication with an authentication method that another could not easily access. Be cautious of all apps downloaded to devices, be sure to only download apps from AppStore or PlayStore. Look through your apps. If there are some that you do not know how they got there and they are not needed, uninstall them.

Watch for possible fake accounts where a person has assumed a fake identity to gain access to you. This false identity may even be in the form of someone you know. Always question the individual to ensure they are who they say they are if you are suspicious.

If you believe you are a victim of cyberstalking, immediately use someone else's computer or device to file a report with local law enforcement, or do so on the FBI's website https://www.ic3.gov/. Also, change all passwords to all accounts. Let them know you do not want contact, and block the individual on social media and your phone. Report them on social media if applicable.

One of the most important things a victim can do is to inform others of what is happening. Remaining silent could cause the problem to go on and the victim's mental health to decline and increase safety concerns. Whether reporting the incident or not, always tell a trusted friend. The more people that are aware, the better. The situation will be known if something more tragic happens to the victim. If the offender attempts to contact the victim's family or friends in any way, they will be aware and better able to decide how to respond.

Record all communications, preferably in print form and cloud storage. Store these in a safe place, with law enforcement or with an attorney.

Further reasons a victim may not seek help:

- They do not understand that what is happening to them is stalking and illegal.
- They Try to pretend that it is not happening.
- A belief that they should be able to deal with the situation, thinking that the stalker will see reason, or not wanting to get the stalker into trouble.
- Fear that others will think they are overreacting or will receive blame for somehow having encouraged the stalker in the first place. The latter is particularly pertinent for those who have had a previous intimate relationship with the stalker, even if it was only brief or just a flirtation.
- They may have fears about how the stalker will respond either to them or those that they care about or love.
- Direct threats from the stalker
- They feel isolated in their plight, believing that nothing can be done to help them or that they do not know where to go.
- Previous requests for help have yet to be addressed.
- Fear of losing their job or the situation becomes complicated when the stalking originates in the workplace.
- They have financial limitations about seeking legal advice or taking time off to seek help.
- Limited options concerning changing their situation, e.g., relocation to safer housing
- Language barriers. (StalkINC, 2023)

Question 5: How can law enforcement or the victim gain an advantage in gathering and maintaining evidence?

As previously stated, keep a record of all communications, preferably in print and cloud storage. Store these in a safe place, with law enforcement or with an attorney. It is necessary to have all evidence of the interactions.

One essential thing is for law enforcement to implement the proper training and have a cyber team available to tackle these cases. Specific training in areas related to cyberstalking would greatly benefit the outcomes of these cases.

As discussed earlier in the paper, some forms of evidence are more acceptable than others, such as mirroring a device. Understand what is and is not acceptable as evidence and limit wasting time accumulating evidence that will not be useful.

For law enforcement to understand the scope of the harassment, they must access the wifi that is used or gain access to the devices. This access allows them to see the entire picture of what is occurring, especially if the stalker is hacking the victim's device and making it appear that the victim is doing things on her own that she is not. The most crucial thing law enforcement can do is monitor and record the instances of abuse before bringing a crime forward with any charges. Doing so after charges or questioning will significantly reduce the amount of evidence that could have been accumulated and likely be the cause for the destruction of the majority of evidence. Any tip-off to the perpetrator will result in extensive destruction of evidence.

Question 6: How is Cyberstalking charged and prosecuted?

The FBI website classifies cyberstalking as a federal crime that “falls under a federal stalking statute as part of the Violence Against Women Act of 2005.” (FBI, 2023) The law

"makes it illegal to use "any interactive computer service or electronic communication service" to conduct activity that places a person "in reasonable fear" of death or serious bodily injury, or that causes or could cause "substantial emotional distress.'"

These actions must be intentional, and if found guilty, Cyberstalking is punishable by up to five years in prison and a fine of $250,000. If the results of the cyberstalking lead to death, a life sentence can be placed on the offender. (FBI, 2023)

Most states charge cyberstalking as a misdemeanor, but it is potentially a felony. It becomes a felony upon fulfilling all the credentials for a misdemeanor which include:

Intent to [harass] [or] [intimidate] [or] [torment] [or] [embarrass] another, he or she makes an electronic communication

[using lewd, lascivious, indecent, or obscene words, images, or language] [or]

[suggesting the commission of any lewd or lascivious act] [or]

[[anonymously] [or] [repeatedly], whether or not a conversation occurs]

[or]

[threatening to inflict injury on the person or property of the person [called] [or] [to whom the electronic communication was made] [or] [any member of his or her family or household]]

AND

[*the person had previously been convicted of any crime of harassment [with the same victim] [or] [member of the victim's family or household] [or] [any person specifically named in a no-contact or no-harassment order]]*

[or]

[the threat was a threat to kill [the person [called] [or] [to whom the electronic communication was made] [or] [any other person.]]

Most states require that charges be filed wherever the crime is committed or where the victim resides. A defendant can be convicted even if the state where he resides does not have cyberstalking laws based on where the charges are filed. Also, other charges may be brought if the state does not have cyberstalking laws. If the crime is sexual, a defendant may need to register as a sex offender. (Johnson, 2022)

If convicted, the penalties for this type of crime are adequate. The issue is convicting the offender first, gathering enough evidence to support the victim's accusations, and utilizing the evidence to result in an actual conviction. Convictions must follow charges in this area to protect the victims and future victims' protection and their trust that when they do report, their doing so will bring about results.

Question 7: The Way We Currently Handle Cyberstalking, is it Effective?

Often charges of cyberstalking require there to be a threat within the communication. However, this has issues, as cyberstalking does not always pose a direct threat. Still, a person's fear is just as valid and can affect their mental health on the same level. In addition, as many criminal behaviorists know, threats are seldom precursors to actions. Criminals rarely provide warnings or "threats" before they commit an act.

Another issue with cyberstalking is that stalkers often enlist third parties to harass the victim. Laws need to be imposed in all states that cover this issue.

Not all states have cyberstalking laws, and some laws only cover specified devices and specified acts on those devices.

The College of Policing researched Police responses to cyberstalking during the Covid-19 pandemic in the UK, and the results from the officers stated that one of the most significant issues with cyberstalking is for the police to understand when a crime has been committed. They also believe that victims are given unrealistic expectations of the outcomes, and 27% of officers stated they found it challenging to understand cyberstalking behavior. (Short, Frost, Bradbury, Bleakley, & Martelozzo, 2022)

The biggest problem with prosecuting a cyberstalker is acquiring adequate evidence against the stalker. The acquired evidence needs to convince a court of the effects then. Cyberstalking needs to be taken more seriously, as the outcome of such can be deadly for the victims or their families. Until one is a victim of this crime, the effects of it can be hard to comprehend. Cyberstalking is a serious crime and should be treated as such in all areas of the US.

Conclusion

Cyberstalking is a crime seeing rapid growth across the US. Many incidences of cyberstalking are never reported due to many factors, the most prominent of which is the victim's faith in law enforcement's ability to handle the situation. A victim is often fearful of her stalker, and she understands that bringing charges against him only further puts her at risk and significantly decreases her safety. A victim needs to feel confident that if she reports, there will be results, and she can regain control of her life and live in peace, something that she has not experienced for years.

Most victims are women between 18-40, and an offender is usually a man. Majority of cases, the victim knows the stalker, and the most seen relationship is that of an ex.

Stalkers fall into five main groups that explain their mindset for stalking behavior, rejected, resentful, intimacy seeking, incompetent suitors, and Predatory. Some intimacy-seeking and incompetent suitors correlate with learning and developmental disorders. However, the other behaviors show a relationship between stalking and personality disorders, most often cluster B disorder. Predatory stalking is the most dangerous form of stalking.

Law enforcement has gained traction in recent years with cybercrime, but they are still behind where they should be in cyberstalking. Law enforcement does not understand what exact circumstances show a cyberstalking crime has been committed. Further training could alleviate this problem.

Awareness about cyberstalking needs to be brought to the public, as many people still are unaware of its existence. Many who know about it do not understand what happened with this crime and how the stalker abuses his victim. In addition, courts and even police should be

made aware of how destructive and damaging this crime is and the potential harm that comes with it.

Understanding the type of person who commits these crimes can aid the criminal justice system. It will aid in researching the problem and finding ways to prevent it before it begins or possibly monitor suspected individuals. Providing therapy or psychiatry to stalkers may eliminate or decrease the instance of the individual committing the crime.

The current consequences against the accused are sufficient if an offender is convicted of cyberstalking. The more significant issue is in gaining Conviction in the first place. Law enforcement needs to work together with the victim to ensure the stalker is brought to justice and also to ensure the victim's safety in the process.

Recommendations

Law enforcement has made considerable advancements in cybercrime; however, they still have a long way to go. Specialized training in cyberstalking and a cyberstalking unit should be a part of all police departments. Officers' training should be well-rounded in cyberstalking. Where they are less confident, such as knowing if a cyberstalking crime has occurred, could be integrated with simulated training to instill their confidence further.

The best way to accomplish the goal of bringing widespread awareness is to start from the ground up. Bringing awareness to the public about cyberstalking through awareness campaigns will be necessary so that all people understand the entirety of this crime. Many do not understand the complexity of what happens during harassment and stalking and how traumatizing the effects can be to the victim.

Realizing the therapy treatment may provide some benefit to stalkers is essential. Certain personalities are unlikely to benefit from therapy as they do not see they have a problem, or they will lie about everything during their sessions. It is still advisable to implement therapy with all individuals as this has been shown to provide more benefits than not.

Educating people on how to protect themselves from cyberstalking is vital for the future of this crime.

Cyberstalking should be a high-level and top-priority crime with its unit and skillsets that departments can train their employees. Also advised is simulated training.

When pressing charges, it is best to wait this out. Once a victim has come forward, collect her evidence, and determine what is needed. Suppose much information is still required

for the prosecution to feel confident. In that case, the victim can allow investigators to silently monitor her internet and cell traffic while collecting the evidence they need to properly bring the case to court. Once the stalker knows that charges may be coming, all evidence will likely be destroyed, so securing this evidence first is critical.

Once charges are filed against the stalker, it becomes essential to protect the victim as she is in the most danger during this period. During this time, it is best to continue monitoring her traffic and provide some form of on-site police protection or a pager she can keep and press if in danger. This type of alarm would notify police without any other threat information and act quickly.

A close team-like connection should exist between the officers and the victim to provide her safety and give her confidence in the officers, as well as allow the officers to do their job better and ensure a conviction of the stalker.

Highly Recommended

To allow better collection and less continuous monitoring by the investigator, a type of software should be created that the victim can install. This software will record (mirror) all events once installed. It can also be interactive, where once a message is received from the stalker, the victim can add this specific instance to an evidence folder. For any incident the victim feels is harassment, the instance could be uploaded into the folder, stored in a cloud, and transferred to the investigator, where he can protect this information, and an outsider cannot transfer it from the investigator's desk. This software or app could also allow signaling where the victim puts a code in at the start of the harassment. A recording session begins and ends with implementing a code, storing this session as necessary in a separate folder. This automatic

storing of signaled events would reduce the need for the investigator to monitor the entire instance from installation to uninstall.

Also important is adding the ability for the investigator to access the device only as a way to monitor remotely. This access would be beneficial in having a witness to the event.

The recommendations contained in this paper are the current recommendations that would make the most considerable impact in the shortest amount of time. Implementation of other recommendations is necessary, but this is an excellent starting point.

References

A Report from the Attorney General to the Vice President. (1999, August). *1999 REPORT ON CYBERSTALKING: A NEW CHALLENGE FOR LAW ENFORCEMENT AND INDUSTRY*. Retrieved from Webharvest.gov: https://webharvest.gov/peth04/20041022072652/http://www.usdoj.gov/criminal/cybercrime/cyberstalking.htm

Brown, C. S. (2015, June). Investigating and Prosecuting Cyber Crime: Forensic Dependencies and Barriers to Justice. *9*(1). Retrieved from https://www.cybercrimejournal.com/pdf/Brown2015vol9issue1.pdf

Brown, S. L. (2012, February 28). *Personality Disorders and Pathology Expert Sandra Brown, MA, Talks About the Mental Disorders Related to Cyberstalking and Online Attacks*. Retrieved from Civilization: https://civilination.org/personality-disorders-and-pathology-expert-sandra-brown-m-a-talks-about-the-mental-disorders-related-to-cyberstalking-and-online-attacks/

Dellazizzo, L., Dugré, J. R., Berwald, M., Stafford, M.-C., Côté, G., Potvin, S., & Dumais, A. (2018). Distinct pathological profiles of inmates showcasing cluster B personality traits, mental disorders, and substance use regarding violent behaviors. *Psychiatry Research, 260*, 371-378. doi:https://doi.org/10.1016/j.psychres.2017.12.006

Dispatch Editorial Board. (2012, June 11). Cyberstalking cases are hard to prosecute. *The Dispatch*. Retrieved from https://cdispatch.com/news/2012-06-11/cyberstalking-cases-are-hard-to-prosecute/

FBI. (2023). *Cyberstalking*. Retrieved from fbi.gov: https://www.fbi.gov/news/stories/sentences-in-separate-cyberstalking-cases-103018#:~:text=Cyberstalking%20is%20punishable%20by%20up,the%20death%20of%20a%20victim.

Fitzpatrick, B. (2023). *PROTECTING AMERICANS FROM CYBERSTALKING*. Retrieved from ALERT!: https://fitzpatrick.house.gov/protecting-americans-from-cyberstalking

Flórez, G., Ferrer, V., García, L., Crespo, M., Pérez, M., & Saiz, P. (2019, July 31). Personality disorders, addictions and psychopathy as predictors of criminal behavior in a prison sample. *National Library of Medicine*. Retrieved from https://www.ncbi.nlm.nih.gov/pmc/articles/PMC6813663/

Grimes, R. A. (2016, December 6). *Why it's so hard to prosecute cyber criminals*. Retrieved from CSO Online: https://www.csoonline.com/article/3147398/why-its-so-hard-to-prosecute-cyber-criminals.html#:~:text=Jurisdiction%2C%20jurisdiction%2C%20jurisdiction,and%20prosecutors%20seeking%20the%20conviction).

Hechler, D. (2021, October). Why it is so hard to prosecute cyberstalking. *Tag Cyber Law Journal: CyberSecurity News*. Retrieved from https://www.cyberinsecuritynews.com/cyberstalking

Johnson, J. (2022, June 29). *Cyberstalking Charges*. Retrieved from freeadvice.com: https://www.freeadvice.com/legal/cyber-stalking-charges/#:~:text=Cyberstalking%20statutes%20usually%20classify%20it,level%20offenses%20by%20other%20factors.

Kaspersky. (2023). *Tips to protect yourself from Cyberstalkers*. Retrieved from Kaspersky: https://usa.kaspersky.com/resource-center/threats/how-to-avoid-cyberstalking

MacKenzie, D. R., McEwan, T., Pathe, M., James, D. D., Ogloff, J., & Mullen, P. (2011). *Impact of stalking on victims*. Retrieved from Stalking Risk Profile: https://www.stalkingriskprofile.com/victim-support/impact-of-stalking-on-victims

Morgan, R. E., & Truman, J. L. (2022). *Stalking Victimization, 2019.* Office of Justice Programs, Us Department of Justice. Bureau of Justice Statistics. Retrieved from https://bjs.ojp.gov/content/pub/pdf/sv19.pdf

Nuccitelli, M. P. (2023). *Cyberstalking Facts and Types of Cyberstalkers*. Retrieved from Ipredator.co: https://ipredator.co/cyberstalking-facts/#:~:text=They%20tend%20to%20lack%20social,increase%20their%20frequency%20of%20contact.

Nuccitelli, M. P. (n.d.). Mind of the Stalker and Cyberstalker. *Academia*, 10. Retrieved from https://www.academia.edu/1195194/Mind_of_the_Stalker_and_Cyber_Stalker

Pueblo County Sheriffs Office. (2023). *Cyberstalking*. Retrieved from Pueblo County Sherrifs Office: https://www.pueblosheriff.com/215/Cyberstalking

Sevens Legal APC. (n.d.). *When Cyber Bullying becomes a crime*. Retrieved from Sevens Legal APC: https://www.sevenslegal.com/blog/when-cyberbullying-becomes-a-crime/1008/

Short, E., Frost, S., Bradbury, P., Bleakley, P., & Martelozzo, E. (2022). *Police responses to cyberstalking during the Covid-19 pandemic in the UK.* London: Sage Public Health Emergency Collection. doi: 10.1177/0032258X221113452

StalkINC. (2023). *Impact of stalking on victims*. Retrieved from Stalking Risk Profile: https://www.stalkingriskprofile.com/victim-support/impact-of-stalking-on-victims

UNODC. (2020, February). *Cyberstalking and cyberharassment*. Retrieved from United Nations Office on Drugs and Crime: https://www.unodc.org/e4j/zh/cybercrime/module-12/key-issues/cyberstalking-and-cyberharassment.html#:~:text=Cyberstalking%20involves%20a%20series%20of,family%2C%20partner%2C%20and%20friends.

Whitemire, T. (2020). The Arrest and Prosecution of Cyber Stalkers: How "Rational" are Criminal Justice Decision Makers? *Department of Sociology*, 105. Retrieved from https://stars.library.ucf.edu/cgi/viewcontent.cgi?article=1150&context=etd2020

WHOA. (2013). *WHOA 2013 Cyberstalking Statistics.* WHOA. Retrieved from http://www.haltabuse.org/resources/stats/2013Statistics.pdf

Wright, R. G. (2020, April). Cyber Harassment and the Scope of Freedom of Speech. *UC David Law Review Online, 33*, p. 26. Retrieved from UC Davis Law Review Online: https://lawreview.law.ucdavis.edu/online/53/files/53-online-Wright.pdf