2020

The Arrest and Prosecution of Cyber Stalkers: How "Rational" are Criminal Justice Decision Makers?

Trisha Whitmire
University of Central Florida

THE ARREST AND PROSECUTION OF CYBER STALKERS: HOW "RATIONAL" ARE CRIMINAL JUSTICE DECISION MAKERS?

by

TRISHA WHITMIRE
B.A. University of Central Florida, 2006
M.S. University of Cincinnati, 2009

A dissertation submitted in partial fulfillment of the requirements
for the degree of Doctor of Philosophy
in the Department of Sociology
in the College of Sciences
at the University of Central Florida
Orlando, Florida

Spring Term
2020

Major Professor: Elizabeth Mustaine

ABSTRACT

The emergence and continuous development of technology continues to create opportunities for people to communicate and keep track of one another. Numerous websites and cellular applications exist that allow individuals to anonymously send messages, track other's whereabouts, or expose private information. Many of these tools, while innocuously created to enhance friendships and make it easier to stay in touch, are being nefariously used to stalk and harass others through electronic means. The rise of stalking using electronic methods, also known as cyber stalking, gravely complicates the ability of law enforcement officers and prosecutors to adjudicate cases of stalking. This study examines the enforcement of cyber stalking cases in Central Florida through the lens of rational choice theory. In particular, the study evaluates the factors present in stalking cases -- specifically cyber cases -- which impact the rational choices made by law enforcement officers and prosecutors to pursue and process cases. The results of the study show that cases of stalking that involve both cyber and face-to-face components had the highest odds of an arrest occurring and/or charges being filed. Additionally, the study shows that cases of stalking, regardless of the method, had higher odds of arrest or charges if the victim took proactive measures to prevent future occurrences of stalking. Overall, the study found that various factors impacted the rational choices made by law enforcement officers and prosecutors in their decisions to move forward and continue pursing stalking cases. A major implication of this study is that victims should take proactive action to prevent stalking in order for cases to move forward in the criminal justice system.

TABLE OF CONTENTS

LIST OF TABLES

CHAPTER 1: INTRODUCTION

The digital age has opened up new and more effective opportunities for people to keep track of one another. We can use social media, GPS, geo-tagging, and a variety of other mediums in order to track other people's whereabouts and activities. The utilization of these new technologies is a double edged sword. It may be acceptable to use technology such as location services when all parties involved consent, for example when friends want to see where the other is located and arrange a meet up. However, this technology may also be used as an unwanted violation of privacy when someone is following the activities and locations of another unbeknownst to them or against their express wishes. Cutting edge technology, offering vast and exciting improvements to our lives also provides numerous, less detectable and understood ways of committing crime and harassing others. In these unfamiliar environments, law enforcement officers are at a significant disadvantage because they fall behind criminals in knowledge and are hampered due to a lagging legal system and law enforcement policies on these new crimes, criminal methods, and tools used to enforce these offenses.

Many benefits to the increasing ease of access to technology exist. For example, parents who utilize GPS can know where their children are by utilizing tracking applications, friends can easily make plans to meet up at a specific location by sharing location data, and relatives can keep in contact from a distance through messaging and photo sharing programs. However, there are also drawbacks to this ease of access through technology. Individuals may choose to use this technology in order to keep tabs on unsuspecting individuals and invade their privacy or harass them from behind the screens of computers or phones. Additionally, some with more malicious motives may go as far as to use cutting edge technology to commit crimes against other people

such as cyber bullying, hacking, and identity theft. One crime in particular has been growing exponentially with advances in technology: cyber stalking (al-Khateeb et al., 2016).

Cyber stalking is typically viewed as an extension of stalking; a new tool or method that is now available and useful for stalkers. This can be seen in most state statutes. For example, in Florida, stalking is defined as "willfully, maliciously, and repeatedly" following, harassing, or cyber stalking another person (FLA STAT. ANN. § 784.048). Stalking goes beyond surveillance, however, and is intended to cause victims to fear for their personal safety (Owen, 2016). Perpetrators of stalking, who use face-to-face strategies, have a wide range of tactics from which to choose to elicit fear in their victims. Stalkers may follow victims in their vehicles, send victims letters or leave notes, and show up at various locations where their victims frequent including work, school, friends' homes, or regular hang out spots. Additionally, they may contact the friends or family of victims, or send photographs showing victims they are being surveilled. In contrast, cyber stalkers have numerous additional methods and tools at their disposal. Cyber stalkers may continuously send text messages, e-mails, or social media messages, make phone calls, or track locations through various cellular phone applications, all from a distance from the victims. Cyber stalkers may also post victims' personal information online, also known as doxing, for strangers to harass victims' on their behalf or post photographs or videos of the victims. Cyber stalking may be its own unique form of stalking, or it may be an extension of more traditional face-to-face strategies.

Stalking legislation in the United States did not begin until 1990 after a young actress, Rebecca Shaeffer, was shot and killed in 1989 by a fan who had stalked her for two years (National Institute of Justice, 1996). Prior to this incident, law enforcement was aware of stalking, but they were constrained because of legal codes that focused on behaviors over threats.

It took the murder of Shaeffer to bring attention to the full extent of the dangers associated with stalking threats that escalate to violence; thus the need for legislation to protect victims. Following the creation of legislation regarding stalking, law enforcement had to increase its understanding of stalking and the typically associated behaviors so they could work to better identify and investigate it. Law enforcement had to learn to evaluate whether the behaviors and threats showed a pattern, whether the offenders posed a threat to their victims, and whether victims' fear was reasonable. With the onset of electronic and virtual technology and the recognition that these offer vast new tools, strategies, and settings by which stalkers can harass their victims, law enforcement has been forced to keep up with the ever changing technological tools available.

Cyber stalking has grown tremendously over the years due to the wide and nearly universal availability of useful tangible and virtual technology. Perpetrators have ready access to tools to effectively, efficiently, and surreptitiously surveille and monitor their victims. Offenders may send emails or text messages, connect with victims via social media or other discussion-based platforms, or utilize tracking software to find locational and personal data. They can easily impersonate or target their victims in the anonymous and faceless world of the internet. These techniques may be used in order to intimidate victims, to continue unwanted contact with victims, or to obtain information that would allow them to stalk their victims in person.

Numerous phone applications exist that provide offenders with locational data and keystroke documentation from victims. These applications can be installed and run as background programs, most of which would be invisible to victims. While marketed towards parents who wish to monitor their children, these applications can be readily misused as tools for stalking. These applications send data electronically to the person monitoring and often include

data such as who users are making or receiving phone calls from, the content of text messages, geographic locations of the user, images taken through the camera or downloaded, and keystrokes. One tracking application, mSpy, refers to itself as the "Ultimate monitoring software for parental control." Other applications, such as Xnspy, do not require the user to have direct access to the target's mobile device. Xnspy allows user to log into the iCloud account of another individual and have the information, including location data, phone calls, and text messages, sent directly to the user. While we may not think twice about parents using this to protect their children, many of us would be shocked and appalled to hear of its' use against unsuspecting or unwilling victims by nefarious others.

One way law enforcement is hampered in their stalking investigations is via the level of anonymity that is possible in the virtual world. Due to this ease of lurking or being incognito, law enforcement is at a severe disadvantage as proving that a specific person is committing cyber stalking is far more difficult and complex than in the face-to-face world. For example, offenders may create social media profiles with fake names and photographs, use prepaid cellular phones that are not specifically tied to individuals, call or text victims using spoofing applications, post information about victims on forums, websites, or discussion boards in order to get third parties to harass victims, or may get friends and family members to send messages from their devices. While the victims may "know" who is committing the offenses, providing the necessary proof to law enforcement may be virtually impossible. And this is really just the tip of the iceberg. With each new gadget, application, or advancement in technology, stalking is easier and the enforcement of it is harder.

Academic research in this area could seriously aid law enforcement in their efforts to stay up-to-date on the typical or newest techniques being used by stalkers, but research on cyber

stalking is still relatively new and underdeveloped (Strawhun et al., 2013). Studies on cyber stalking often focus on the similarities and differences between face-to-face stalking and cyber stalking (Cavezza & McEwan, 2014), discussions on whether cyber stalking is a type of stalking or a different crime altogether (Grabosky, 2001; Brown, 2015; Lupsha 1996; Zhigang, 2011), how cyber stalking has evolved due to advances in technology (Shimizu, 2013; Strawhun, Adams, & Huss, 2013), and the the laws attempting to protect victims of stalking (Hazelwood & Koon-Magnin, 2013; Chik, 2008). Other studies examine the issues with investigating and prosecuting cyber-crimes due to user anonymity and jurisdictional issues (Brown, 2015; Geach & Haralambous, 2009; D'Ovidio & Doyle, 2003). The present study extends these contributions to the cyber stalking literature by providing a comprehensive examination of the factors that influence arrest and prosecution of stalkers, both cyber and face-to-face. Additionally, the present study will provide a detailed description of the tools and technology used by cyber stalkers and how these impact the decisions prosecutors and police officers make when processing stalkers.

One theory particularly apt at guiding the analyses of law enforcement and prosecutor decision making is rational choice theory. While typically used to explain the behaviors of offenders, rational choice theory states that individuals do a cost and benefit analysis prior to making certain decisions about crime commission (Cornish & Clarke, 1987). In this view, this choice is a rational, calculated analysis made by active agents who consider both the potential risks and rewards of crime (Clarke & Cornish, 1985).

It stands to reason, though, that other individuals involved in the criminal justice system may also utilize a cost-benefit analysis when making choices about offenders or processes. In other words, law enforcement officers may choose whether or not to arrest an offender of cyber

stalking based on cost-benefit analysis of the information provided by the victim and any available witnesses. Additionally, prosecutors may also choose whether or not to move forward with the prosecution of cyber stalking cases by analyzing the costs and benefits based on the evidence and the likelihood of a plea deal or guilty verdict. Theoretically, we should expect victims to make behavioral decisions to cope with their on-going victimization. It also should happen that victims provide or withhold cooperation based on the cost-benefit assessment.

In this study, I will extend the use of rational choice theory to other criminal justice actors and their actions during the criminal justice process: the patterns of action made by law enforcement officers on whether or not to arrest offenders and prosecutors on whether or not to charge cyber stalking offenders with a crime or not. Also, theoretically victims would behave in understandable ways when making decisions about how to react to their cyber stalking victimization and whether or not to participate in the prosecution of their stalker. Additionally, this theory will be utilized to describe the tools and strategies stalkers use on their victims.

As rational choice theory was developed as an explanation of criminal decision making, this application will be a unique approach. By extending the application of rational choice theory to other actors in the criminal justice system, the present study considers the rationality of decisions surrounding arrest, prosecution, and those that victims make about their participation in the criminal justice process. It need not be limited to the thinking about the commission of crime. This extension will have implications for the examination of other criminal justice participants such as the reporting behavior of victims, the use of discretion by law enforcement officers, or the strategic decisions made by defense attorneys.

In sum, this study will examine cyber stalking cases reported to law enforcement agencies in Central Florida. The purpose of the study is to determine whether the variety of cyber

offenses and cyber strategies utilized by offenders as well as the actions and reactions of victims impact arrests and prosecutorial decisions. Specific objectives are: 1) To identify strategies being used by cyber stalking perpetrators, 2) To identify the factors that influence arrest and prosecution behavior, and 3) To investigate the role the victim plays in cyber stalking prosecution.

Offenders of cyber stalking have a number of tools at their disposal to communicate with and track their victims. The tactics used by the offenders and the reactions of the victims may influence the rational choices law enforcement officers and prosecutors make when deciding whether or not to pursue charges or stalking against offenders. The results of this study will show how the factors involved in the cases impact the rational choices of the various players within the criminal justice system and how the system responds to cases of cyber stalking. This is an important segue for the literature in this area. If we increase our understanding of stalking patterns in locations, strategies, and technologies, researchers, community members, and criminal justice actors can work together to share knowledge, thereby increasing the “benefit” side of the policing and prosecutorial decision making considerations.

CHAPTER 2: LITERATURE

Cyber stalking research is underdeveloped, most likely because lawmakers and law enforcement officers are still learning about it themselves. This chapter explores research on several areas of cyber stalking beginning with how cyber-crime and cyber stalking are defined and moving toward discussing the differences between cyber stalking and face-to-face stalking. The literature cited also covers the prevalence of cyber stalking, the impact cyber stalking has on victims, and the barriers to prosecution. In addition, the literature covers the tools and methods employed by offenders of cyber stalking and strategies used by victims to prevent its' occurrence.

Defining Cyber Stalking

Prior to defining the specific crime of cyber stalking in this study, one must first define the broader umbrellas of crime under which cyber stalking falls: stalking, harassment, and cyber-crime. Additional complexity gets introduced when scholars debate the nature of cyber-crime. For example, is cyber-crime a distinct type of crime or is it the same old crime being committed in a new location or via different tools (Diamond & Bachmann, 2015; Cavezza & McEwan, 2014). This debate is still ongoing.

Cyber-crime is defined by scholars as "offenses that are committed against individuals or groups of individuals with a criminal motive to intentionally harm the reputation of the victim or cause physical or mental harm, or loss, to the victim directly or indirectly, using modern telecommunication networks such as Internet (networks including chat rooms, emails, notice boards and groups) and mobile phones (Bluetooth/SMS/MMS)" (Halder & Jaishankar, 2012).

More specifically, stalking in Florida is defined as “willfully, maliciously, and repeatedly” following, harassing, or cyber stalking another person (FLA STAT. ANN. § 784.048). In the same statute, harassment is defined as “to engage in a course of conduct directed at a specific person which causes substantial emotional distress to that person and serves no legitimate purpose” (FLA STAT. ANN. § 784.048).

On one side of the debate, Grabosky (2001), contends that cyber-crimes are simply traditional forms of crime facilitated by technology. In this view cyber-crimes are the same as street and white-collar crimes, offenders simply use technology to assist in their perpetration (Grabosky, 2001). Grabosky (2001) also suggests that the motivations behind cyber-crimes mirror those of traditional crimes, including greed, lust, and revenge.

Other researchers agree with the view that cyber-crime is similar to traditional forms of crime. To elaborate, Brown (2015: 57) stated, “cyber-crime is merely a sub-set of conventional crime where ICT’s (information and communication technologies) are used as a vehicle or tool to commit traditional criminal offenses” (Lupsha, 1996; Zhigang, 2011). Other researchers suggest that cyber-crimes are extensions of traditional crimes (Dogaru, 2012; Davis, 2011; Sheridan & Grant, 2007; Spitzberg & Hoobler, 2002).

On the other side of the debate are researchers who state cyber-crimes are completely different from traditional crimes (Furnell, 2002; Wall, 1999; Yar, 2005; Katyal, 2001; Lucks, 2004). Proponents of this side of the argument point out that while some cyber-crimes may be similar to conventional crimes, others would not exist without technology (Furnell, 2002). These crimes would be distinguished whether they are computer assisted or if they are computer focused (Furnell, 2002). For example, crimes such as stalking, bullying, theft, and fraud may occur either with or without technology and would be considered computer assisted. However,

crimes such as hacking, piracy, and malware only exist in the cyber world, indeed, can only exist in the cyber world due to the presence of certain cyber-only elements.

Researchers also contend that cyber-crime is a distinctive form of crime due to the types of individuals who commit these crimes. According to Dogaru (2012), offenders of cyber-crimes are different than offenders of more traditional crimes and do not fit the heretofore "typical criminal" typologies we have previously understood. This may be due to the increased anonymity of offenders in cyber space, which may reduce the likelihood that offenders will be caught and punished for their crimes (Katyal, 2001; D'Ovidio & Doyle, 2003). It may be that cyber criminals need more specialized knowledge that is harder to attain. Cyber criminals may also be distinguished from more traditional criminals in the ready availability of much of the necessary tools, but also the expense involved with much of the technology. Even so, those committing crimes online may be just like more traditional criminals in that they believe they will never get caught (Katyal, 2001).

The cyber-crime debate brings up the same questions regarding cyber stalking: is cyber stalking a new crime separate from stalking or is it an extension of stalking? Both federal and state governments in the US, have attempted to address the issues arising with the different technologies available for stalkers through the legal system by creating laws that identify behaviors distinctive to cyber stalking. The federal government first addressed cyber stalking in section 2261A(2)(A) of the Violence Against Women Act (VAWA) as an extension of the stalking statute previously covered. The amendment, added in 2006 during VAWA's reauthorization, states:

> Whoever –
>
> ….
>
> (2) with the intent to kill, injure, harass, intimidate, or place under surveillance with intent to kill, injure, harass, or intimidate another person, uses the mail, any interactive computer service or electronic communication service or electronic communication system of interstate commerce, or any other facility of interstate or foreign commerce to engage in a course of conduct that –
>
> (A) places that person in reasonable fear of the death of serious bodily injury to a person described in clause (i), (ii), or (iii) of paragraph (1)(A); or
>
> (B) causes, attempts to cause, or would be reasonably expected to cause substantial emotional distress to a person described in clause (i), (ii), or (iii) of paragraph (1)(A), shall be punished as provided in section 2261(b) of this title.

States have also added cyber provisions to their statutes. This is typically accomplished in one of three ways: the creation of specific laws related to cyber stalking, amendments to stalking laws that include cyber stalking components, or through the application of unrelated laws to cyber stalking cases (DeMatteo et al., 2017; Vasiu & Vasiu, 2016). States vary on a number of issues regarding how they address cyber stalking in their laws. First, some states, such as Ohio, have only one statute that includes cyber stalking (OHIO REV. CODE ANN § 2903.211, 2014) while others, such as Michigan, have multiple statutes under which cyber

stalking behaviors would fall (MICH. COMP LAWS ANN. §§ 750.411h, 2016; MICH. COMP LAWS ANN. §§ 750.411i; 2016; MICH. COMP. LAWS ANN § 750.411s, 2016; DeMatteo et al., 2017). States also differ in whether they put cyber stalking under the category of a criminal offense or a civil action (DeMatteo et al., 2017). The majority of states consider cyber stalking to be a criminal offense, but some, such as California consider it to be a civil matter (CAL. PENAL CODE § 422, 2011; DeMatteo et al., 2017). Those that consider cyber stalking to be a criminal offense also differ on whether they classify it as a felony, misdemeanor, or both (DeMatteo et al., 2017).

Other areas where states differ regarding their statutes are on the intent and actions of the perpetrators of cyber stalking. Some states require that the offender must intend for the behavior to provoke specific reactions out of the victim, such as fear, emotional distress, or intimidation, while other states make no reference to this requirement (DeMatteo et al., 2017). Most states also require that in order for behaviors to be labeled as cyber stalking, they must be repeated more than one time, while only a few states do not explicitly give this requirement (DeMatteo et al., 2017).

State statutes also vary in how they define cyber stalking. Florida is one of the states that has a non-specific cyber stalking law, meaning it does not stand alone but falls under the category of stalking (DeMatteo et al., 2017). So, in Florida, cyber stalking is clearly defined. There, the law defines cyber stalking as “engag(ing) in a course of conduct to communicate, or to cause to be communicated, words, images, or language by or through the use of electronic mail or electronic communication, directed at a specific person, causing substantial emotional distress to that person and serving no legitimate purpose” (FLA STAT. ANN. § 784.048(d), 2012; DeMatteo et al., 2017). As this study takes place in Florida and follows cases handled by law

enforcement and prosecution under Florida law, heretofore this is the definition of cyber stalking to which the present study relies.

Even though scholars are not in complete agreement about the legal and definitional issues surrounding cyber stalking, they are advancing our knowledge about this emerging and ever-changing crime. The following section considers what we know about cyber stalking and which important gaps still exist.

Cyber Stalking Versus Face-to-Face Stalking

Just as debate exists for practitioners as to whether cyber-crimes are new and distinct forms of crimes or are extensions of more traditional crimes in the law, social science scholars have the same debate. Researchers maintain that the psychological outcomes of cyber stalking can be just as harmful as face-to-face stalking (Maple, Short, & Brown, 2011; Cavezza & McEwan, 2014), but the question still remains as to whether cyber stalking stands alone or falls under the stalking umbrella. The answer to this question is important because it tells researchers how to study cyber-crime in the future. It also can benefit law enforcement and prosecutors in their investigative and prosecutorial efforts.

Those who argue that cyber stalking is a new type of crime often speak of what the Internet offers offenders that face-to-face stalking does not. Meloy (1998) suggests there are elements in the virtual world not found in face-to-face interactions. Due to these unique aspects of technology and the cloud, some researchers suggest that individuals who cyber stalk would not engage in face-to-face stalking (Menard & Pincus, 2012, Cavezza & McEwan, 2014). Cyber stalkers, therefore, are distinct from face-to-face stalkers. According to Meloy (1998), the

Internet offers four unique elements for stalkers: (1) a lack of social constraints inhibiting aggression; (2) a lack of sensory stimuli leading to greater fantasy in the offender; (3) the opportunity for deception; and (4) the potential for surprise when they realize that their involvement with the victim does not conform to what they imagined (Cavezza & McEwan, 2014, p. 957). Researchers hypothesize that these unique elements of the Internet may encourage individuals who would not stalk face-to-face to do so online (Menard & Pincus, 2012).

Some of the earliest research on cyber stalking suggested that offenders of cyber stalking were "emotionally disturbed loner(s) seeking attention and companionship through cyberspace" (Stephen, 1995, p. 27). Additional research on cyber stalking perpetuated the loner stereotype by finding that cyber stalkers were more likely to have an Internet 'addiction' and use explicit materials, often had no official criminal history, and had a higher number of victims, particularly those of younger ages (Lucks, 2004). Due to these results, Lucks (2004) suggested that cyber stalking was a completely separate crime from face-to-face stalking.

Despite the preponderance of research indicating that cyber stalkers and face-to-face stalkers were different types of individuals with distinct behaviors, the other side of the argument still persists. These proponents suggest that the differences between the stalking typologies are more minor than earlier research suggested (Sheridan & Grant, 2007; Cavezza & McEwan, 2014). Sheridan and Grant (2007) found that the only significant difference between the cyber stalking cases and the other typologies was the relationship type. Namely, those who were stalked only online were more likely to be stalked by strangers or acquaintances while those stalked face-to-face were more likely to be stalked by ex-partners (Sheridan & Grant, 2007).

However, in another study cyber stalkers and face-to-face stalkers had approximately the same number of victims, the same level of education, and the same likelihood of using violence

(Cavezza & McEwan, 2014). The method of stalking did not result in the greatest differences in behaviors or characteristics, but the motivations behind the stalking played the largest role, including wanting to harm the victims or wishing to communicate with them (Cavezza & McEwan, 2014). Therefore, cyber stalkers and face-to-face stalkers with the same motivations will have similar characteristics and similar stalking behaviors (Cavezza & McEwan, 2014).

While the earliest research suggested that the individuals committing cyber stalking were loners who would not engage in face-to-face stalking without the safety of the computer (Stephen, 1995), more recent research seems to suggest that cyber stalkers and face-to-face stalkers may not be all that different (Sheridan & Grant, 2007; Cavezza & McEwan, 2014). Instead of becoming a new crime and attracting a new breed of criminals, the Internet instead may have become a new "location" for their criminal endeavors and/or a new tool to increase their effectiveness and further concealing their identities.

Prevalence of Cyber Stalking

As stated previously, cyber stalking is still a relatively new issue and therefore is understudied in research (Strawhun et al., 2013). Researchers have attempted to quantify the prevalence or frequency of cyber stalking, however, given the variety of methods of stalking that may be included in these studies, the numbers vary greatly (Stawhun et al. 2013, Reyns et al., 2012). Reyns, Henson, and Fisher (2012) reviewed literature in their study and found that depending on the sample and methodology the prevalence rates of cyber stalking varied between 1% and 82% of respondents having been the victim of cyber stalking in their lifetimes.

A particular study that attempted to tackle prevalence was conducted by Fisher, Cullen, and Turner in 2002. The researchers conducted a study not strictly exploring cyber stalking experiences but including victimization questions with cyber components. The study showed that 13.1% of the college students were stalked a minimum of one time since the beginning of the school year, while 12.7% experienced two or more incidents, and 2.3% experienced three or more (Fisher et al., 2002). In examining the cyber elements of this study, 77.7% of the incidents were through the telephone and 24.7% of the incidents were through e-mail (Fisher et al., 2002).

Similarly to the 2002 study by Fisher, Cullen, and Turner, the Supplemental Victimization Survey (SVS), a survey conducted in 2006 as an extension of the National Crime Victimization Survey (NCVS), examined stalking behaviors that included cyber components (Catalano, 2012). The SVS was conducted with individuals age 18 and over who had completed the NCVS in 2006. Findings included that for victims of stalking, unwanted phone calls and messages were the most common strategies used by offenders (Catalano, 2012). Specifically, 66.7% of stalking victims experienced unwanted phone calls and messages (Catalano, 2012). Other stalking techniques included posting information or spreading rumors about the victim, which 36.3% of victims reported experiencing, however this category included both cyber and non-cyber components (Catalano, 2012).

In another college aimed study, Reyns, Henson, and Fisher (2012) found that 40.8% of students had experienced cyber stalking at some point during their lives up to that point. This study found the following: 23.3% experienced repeated unwanted contacted after being asked to refrain, 13.6% experienced repeated unwanted sexual advances, 20.1% experienced unwanted harassment, 4.2% experienced repeated threats of violence (Reyns et al., 2012). This study found a high rate of cyber stalking victimization; however, it is important to point out that it included

online pursuit in addition to identity fraud, which accounted for 12.1% of the victimization (Reyns et al., 2012).

With prevalence rates similar to the previous study, Deßing, Bailer, Anders, Wagner, and Gallas (2014) found that over 40% of the social networking users surveyed had been harassed online at least once during their lives. Continuing their research, Deßing and colleagues added in two additional components to measure cyber stalking prevalence: duration of greater than two weeks and harassment that induced fear (Deßing et al., 2014). When those additional components were additionally considered, the prevalence of cyber stalking dropped from over 40% to 6.3% (Deßing et al., 2014). These studies alone showed prevalence rates varying greatly depending on the operationalization of the key legal concepts being evaluated.

Researchers studying the prevalence of cyber stalking have also sought to examine the impact on victims. Research shows that some victims experience psychological impacts such as fear, anxiety, and frustration (Smith, 2010), while other victims become angry and annoyed (Ngo & Paternoster, 2016). Deßing et al. (2014) found that two thirds of the victims in the study had sleep disturbances since their victimization and 16% were receiving counseling or therapy. However, as the majority of the victims experienced both cyber stalking and face-to-face stalking, it is impossible to tell which type caused the psychological difficulties faced by the victims.

Bocij (2003) measured the psychological impact cyber stalking has on victims using a scale of 1 to 10. The average level of distress caused by the incidents was a 7.16, with 22.8% of the respondents scoring a 10 (Bocij, 2003). In addition, the participants with more computer knowledge reported less distress due to their cyber stalking victimization (Bocij, 2003). The

research clearly shows that cyber stalking negatively impacts victims, however more extensive research may need to be done in order to determine the extent of the problem.

Another important issue in cyber stalking research concerns factors put individuals at greater risk for victimization. A study by Holt and Bossler (2008) found that simply being online, even for great amounts of time, does not make individuals more likely to be harassed; but, being online in environments that place potential victims with motivated offenders, such as chat rooms and instant messaging, does increase the chances of victimization. Holt and Bossler (2008) found that individuals who spent greater amounts of time in chat rooms and on instant messaging applications made them more likely to be harassed online. Research has also shown that individuals who visit more social networking sites are more likely to be cyber stalked or bullied (Kraft & Wang, 2010; Strawhun et al., 2013).

There is still much research to be done in the area of cyber stalking. The prevalence rates of cyber stalking vary widely depending on the sample and methodologies used in the studies (Stawhun et al. 2013, Reyns et al., 2012). In addition, the impact on victims remains unknown due to the overlap of cyber stalking and face-to-face stalking. While the research on cyber stalking and cyber-crime in general is expanding, we are lacking in validity studies and gaps are still prevalent. One area we particularly need to explore is how the methods utilized by offenders, the actions taken by and level of cooperation of victims, and the factors impacting the considerations surrounding arrest and prosecution decisions in cyber stalking cases. The current study seeks to fill a few of these research gaps.

Cyber Stalking Methods & Tools

Offenders of cyber stalking have a wide variety of technological tools at their disposal. Every day new software and devices are being created that advance individual's abilities to communicate with one another. Technology gives individuals the opportunity to communicate with others around the world with just a click of a button. As technology continues to advance, the options cyber stalkers have to communicate with victims expand. Individuals who cyber stalk others may choose to utilize communication platforms that are tied to their identities. E-mail addresses, phone numbers, social media accounts, and other usernames may provide victims with the identities of the offenders. The identities of offenders may be easily discernible if the information includes the offenders' names or if the victims and offenders have previously communicated with each other using the same methods.

However, offenders may choose to utilize various technologies in order to hide their identities from victims and from law enforcement with little effort. Mobile device applications such as SpoofCard, TraceBust, and Second Phone Number, allow users to change their phone numbers when making phone calls or sending text messages, also known as spoofing (Landhuis, 2018). These applications, and many others, make phone calls or text messages appear as though they are coming from different phone numbers, including numbers of individuals known to victims. SpoofCard markets the application with "Easily disguise your caller ID" and allows callers to call victims with the caller ID showing any number of their choosing. Additionally, SpoofCard allows users to manipulate their voice, background noise, and whether the victim's phone rings or if the call goes straight to voicemail. These applications allow offenders to contact victims if their original phone numbers have been blocked and may increase the likelihood that

victims will answer phone calls due to their familiarity with the phone numbers (Landhuis 2018).

Offenders of cyber stalking may purchase track phones with new phone numbers to make calls or send text messages. Offenders may also choose to create new e-mail addresses or social media accounts with different names, photographs, and identifiable information in order to disguise their identities (Landhuis, 2018). In addition, offenders may utilize anonymous remailers that remove virtually all trace of electronic mail transmissions (D'Ovidio & Doyle, 2003). These remailers "strip identifying information from the email header and erase any transactional data from servers that would enable law enforcement to trace the message back to the author" (D'Ovidio & Doyle, 2003:16).

As technology exists to hide the identities of offenders, numerous applications and tools also exist to track the behaviors of victims. Applications such as mSpy, Spyzie, and FollowMee may be installed onto the mobile devices of victims and used by offenders to track their whereabouts. These applications along with many others run in the background of cellular devices unbeknownst to the victims. Tracking applications include a variety of tools including location data, keystrokes, phone calls, text messages, and more. These applications are often marketed towards parents as a way to keep track of their children and to monitor their activities, but may be used by cyber stalkers to watch their victims. Some of the tracking applications, such as Xnspy, do not require offenders to have physical access to the victims' mobile devices to install the software. Offenders of cyber stalking who live in close proximity to their victims may also purchase magnetic tracking devices that can be attached to the bottom of the victims' vehicles. These devices often come with tracking software that sends location data from the vehicle to the offenders' mobile devices (Landhuis, 2018).

Offenders may also track the locations of victims through location data saved on photographs. Photographs taken on cellular phones may include Exchangeable Image File (EXIF) data that includes information such as shutter speed, aperture, date and time, and location data including longitude, latitude, and altitude. Photographs can be downloaded by offenders and analyzed through EXIF data applications, such as EXIF Viewer, which place the location the image was taken on a map. This data allows offenders to know the locations in which photographs were taken by the victims. For example, children residing at a local domestic violence shelter with their mother took photographs of artwork they had created and shared the photographs to social media. The children's father, who had abused their mother and from whom they had fled, used EXIF data from the images shared by the children and found the confidential location of the family (Landhuis, 2018).

Cyber stalking offenders may choose not to engage with their victims directly. Some offenders may post information about their victims on social media and other public websites in order to encourage third party individuals to contact the victims directly. In some cases, offenders have made advertisements on websites and profiles on dating websites using the contact information of victims and photographs of either the victims themselves or other individuals. These advertisements and profiles may state that victims are interested in finding sexual partners or that they have items to give away or sell. By releasing the contact information of the victims, also known as doxing, offenders allow third parties to harass the victims on their behalf without ever needing to make direct contact themselves (Landhuis, 2018).

Cyber Stalking Prevention Strategies

While offenders of cyber stalking have a large number of tools available to stalk victims, victims have only limited tools available to stop or prevent these behaviors. Victims of cyber stalking may choose to block offenders on cellular devices, social media accounts, and e-mail. However, offenders may utilize other phone numbers, social media accounts, or e-mail addresses that get around the blocking. As previously mentioned, if offenders utilize spoofing applications, the victims' mobile devices do not recognize that the users have been blocked. Victims may choose to make their social media accounts private or create new accounts and change their identifying information, including name, photographs, and contact information. Victims may also choose to change their phone numbers, e-mail addresses, or social media account login information (Landhuis, 2018).

In the event that victims of cyber stalking are unaware of who is perpetrating the behaviors, victims may utilize tools to unveil information about the users. Numerous websites exist to reveal the identities of individuals for a fee, including Spokeo, Intelius, and PeopleFinders. These websites allow users to enter the phone numbers, e-mail address, or names of individuals and provide additional contact information, along with additional personal data. A mobile device application, TrapCall, may also be used by victims of cyber stalking to provide information about the offenders. TrapCall unblocks phone numbers that have been blocked by the offenders, providing the victims with the phone number of the offenders. TrapCall only works, however, if the offenders have blocked their phone number, not if the individuals have utilized spoofing applications (Landhuis, 2018).

Victims who know the identities of cyber stalkers may be able to utilize the court system to prevent future occurrences. Victims may file for injunctions for protection, also known as restraining orders, against offenders of cyber stalking. The injunction for protection, if granted, makes future contact between the victim and the offender a criminal offense for the duration of the injunction. However, in order to file for the injunctions, victims must know the names and residential locations of offenders so that injunctions can be served.

Technology offers both offenders and victims of cyber stalking with numerous tools. Offenders of may choose to engage in cyber stalking either in ways that allow victims to know their identities or anonymously. Alternatively, victims may choose to utilize resources to block offenders from making contact or to attempt to identify the offenders. The on-going advances in technology will most likely continue to make communication between individuals easier, which in turn may provide additional opportunities for cyber stalking offenders to contact or track victims.

Law enforcement may provide victims of cyber stalking with tools and suggestions to keep records to assist in the investigation and prosecution of their case as well as safety plan with the victims. Victims of cyber stalking may utilize incident logs in order to track the date, time, method, and content of the stalking behaviors (Landhuis, 2018). In addition, victims may benefit from documenting the way the incidents made them feel, as emotional distress is a key component of cyber stalking legislation (Landhuis, 2018). Law enforcement officers may also discuss the safety implications of strategies to prevent future occurrences of cyber stalking, as the prevention of tactics may cause offenders to escalate their behaviors.

Barriers to Prosecution

Victims of cyber stalking play a valuable, if not essential, role in prosecution and many may be unaware of how important their role is. Some victims may choose to move forward with assisting prosecution, while others may start that way but change their minds, either out of fear or for other reasons. Some victims, who feel law enforcement has not done much for them may be hostile and uncooperative from the start. Nevertheless, once victims have reported instances of cyber stalking, the power is out of their hands regardless of their desire to participate in the prosecution or not. However, as stalking cases rely heavily on the amount of fear victims felt during the offenses, prosecutors may choose not to move forward if the victims back out or are not fully forthcoming. Victims may also decide to be highly involved in cases and become extremely upset if prosecutors decide not to move forward. However, while victims and even prosecutors may want to move forward with the cases, they may be limited in doing so due to barriers caused by the law, by the available evidence or by honest confusion regarding the offender identities.

While the United States government and the majority of states have created laws against cyber stalking, prosecuting these crimes entails confronting a whole new and complex set of issues. Aside from those involving the victims, the major barriers in these cases appear to be regarding jurisdiction (Shimizu, 2013), anonymity (D'Ovidio & Doyle, 2003; Brown, 2015), obtaining records from Internet service providers and cell phone carriers (Brown, 2015), and proving that it was the offender who was using the technology at the time of the offense rather than someone who had legally or illegally accessed that person's account or technology items and committed the crime unbeknownst to the offender (Shavers, 2013; Brown, 2015).

Jurisdiction plays a role in charging a suspect in cyber stalking cases. As cyber-crime allows the offender to remain at a remote location, the offender may not be in the same geographical area as the victim. This causes problems with law enforcement officers and prosecutors determining which location has jurisdiction over the crime (Shimizu, 2013). Shimizu (2013:129) states that the "absence of territorial borders in cyberspace clouds the imposition of traditional territorial concepts to the Internet." Laws in some states dictate that the area in which the offense is committed, or where the offender is located at the time of the crime, holds jurisdiction (Shimizu, 2013). However, other states dictate that the victim's location determines jurisdiction (Shimizu, 2013). Jurisdiction may be even more difficult to determine if the offender did not send direct messages at a specific target (Shimizu, 2013). These conflicting laws sometimes result in confusion as to which location should handle the investigation and prosecution of the crime, meaning that some of these cases may be lost in the shuffle.

Both the offenders and the victims themselves may cause barriers in the investigation of cyber-crime cases. Victims are sometimes reluctant to involve law enforcement due to the belief that cyber-crimes are not taken seriously and that law enforcement is not capable of catching the offender (Brown, 2015). If victims choose not to report the crimes, then offenders may victimize other individuals over time. Additionally, many laws on cyber stalking require a substantiated, credible threat to the victim (Brown, 2015). Unfortunately, in cyber stalking cases, the offenders may not make direct threats towards the victims (Brown, 2015). This may increase the odds of these types of cases being dropped.

Another major barrier in cyber-crime cases is due to the anonymous nature of cyber space (D'Ovidio & Doyle, 2003; Brown 2015). Brown (2015) points out that the anonymity afforded to offenders of cyber-crime makes apprehension extremely difficult. Individuals online have the

ability to use fake social media accounts, e-mail addresses, or phone numbers to hide their identities. As mentioned previously, numerous applications exist to manipulate the information that is shown to victims, making it difficult for victims, law enforcement officers, and prosecutors to prove who is committing the offenses. Another barrier pointed out by Brown (2015) is the reluctance of Internet service providers and cell phone carriers to release information to law enforcement that may assist in the identification of offenders. Oftentimes, the information of additional users would be released along with the accused offenders, and these providers are required to maintain the privacy of other users (Brown, 2015). Internet service providers differ in their definitions of subscriber records and transactional records; with the former requiring a subpoena and the latter requiring a search warrant (D'Ovidio & Doyle, 2003). These records are often necessary in order to prove these cases and are very time consuming to obtain (D'Ovidio & Doyle, 2003). These issues could make it difficult for prosecutors to obtain the evidence they need to move forward with trials.

The greatest barrier in prosecuting cyber-crime is the need to place the suspect "behind the keyboard" (Brown, 2015). While law enforcement may be able to determine which pieces of technology were used to commit cyber-crimes, successful prosecution requires that they also prove that the particular defendant was the one using the technology at the time of the crimes (Brown, 2015). In the event that offenders share technology with family, friends, roommates, etc. or utilize public access computers or no contract cellular phones, proving this may be difficult, if not impossible (Brown, 2015). Brown (2015) discussed the potential for circumstantial evidence to assist in showing that the suspects were in fact the offenders of cyber-crimes.

Shavers (2013) states that over the years, as technology advances, it will become in some ways easier and in other ways more difficult to "place a suspect behind a keyboard." Shavers

(2013) suggests that the new operating systems will create more metadata, meaning that more backup files will be made and more evidence will be available. Additionally, he states that hardware and software applications will be developed that will make collecting evidence significantly easier than before (Shavers, 2013). However, he also says that encryption of data, remote control of systems, open wi-fi hotspots, and the ability to easily duplicate data will also make it more difficult (Shavers, 2013).

Typically, when special knowledge or skill is required to investigate or enforce a crime, special units are formed so officers can be trained in the particular and complex knowledge that is required (i.e. White Collar Crime Division, Domestic Violence Unit, Narcotics Enforcement, etc.). At this point, most law enforcement agencies do not have or have newly installed special, highly trained cyber units to investigate these types of crimes (Willits & Nowacki, 2016). Without these specialized units or advanced training, law enforcement officers may not have the resources necessary to provide prosecutors the evidence they need to successfully adjudicate these cases.

The literature shows that cyber stalking is a very difficult crime to prove. Law enforcement officers have to deal with jurisdiction issues and obtaining records from Internet service providers and cell phone carriers and often do not have up to date technological training or the equipment necessary to place an offender behind the keyboard. Without being able to determine that suspects were the ones operating the equipment at the time it was being used to cyber stalk individuals, prosecutors are often unable to move forward with cyber stalking cases. Given this, the literature also shows that investigative and prosecutorial decisions are made based on rational deliberations involving the cost or effort of moving forward with the case

as compared to the likelihood or receiving the benefit or reward of winning the case. Herein lies the foundation of rational choice theory, even when it examines actors other than offenders.

CHAPTER 3: THEORY

Several theories of crime have recently been applied to various forms of cyber-crime. Researchers have not yet reached conformity regarding whether or not these theories apply to crimes that take place in the virtual world in addition to those in the real world for which the theories were developed. While each of the theories has some challenges when being applied to cyber-crime, each also appears to have some successful applications for explaining how and why these crimes occur.

Social learning theory has been applied to cyber-crime by multiple researchers. Social learning theory suggests that individuals learn behaviors through either direct experience or by observing others and through the rewards or punishments associated with the behaviors (Bandura, 1971). As stated by Holt, Burruss, and Bossler (2010) and Higgins (2006) one reason that social learning theory applies well to cyber-crime is that individuals perpetrating these behaviors must first learn how to use the technology. While the crimes occur in the virtual world, the learning of behaviors may take place both online and offline. Virtually, offenders may learn how to commit crimes such as hacking through blogs, videos, discussion boards, and chat rooms. Cyber stalking offenders, for example, may learn how to create fake profiles, mask IP addresses, install GPS tracking software through malware, access webcams and microphones remotely, and bypass defensive measures such as blocked messages through the online community. Offline, potential hackers may learn through books. Offenders may also learn how to stalk or harass individuals through both online and offline mediums. These individuals may witness stalking techniques, bullying, and harassment in person and translate those behaviors virtually. Additionally, they may see these crimes taking place online and repeat the behaviors themselves.

Another aspect of social learning about which researchers disagree is whether virtual relationships are strong enough to influence individuals through socialization, learning, or differential association. Similarly to Holt and Bossler (2008) and Bocij (2004), it could be argued that virtual relationships may be just as strong as relationships that take place in person. Individuals meet virtually, converse regularly, and share personal information that allows them to connect with each other. They may "talk" to each other online frequently due to the numerous avenues available to communicate virtually. Even so, another factor to consider is that relationships probably do not solely take place online or offline, but likely involve a combination of mediums that allow the relationship to build and become more strongly attached. In today's society, it would be difficult to say that we build our relationships solely in person when we frequently utilize technology to communicate. What has inevitably become the norm is when individuals meet, they exchange email addresses, social networking account names, and mobile phone numbers, thereby opening up numerous ways to connect and interact both on and off-line.

Cyber space, much like the real world, allows individuals to seek out peers with similar interests (Holt et al., 2010). Just as people may join a club or even a gang to associate with peers that share the same interests, online, individuals may join chat rooms, discussion boards, online groups, and blogs to find peers. Also similar to being face to face, individuals are more likely to seek out online peers with deviant interests if they themselves hold favorable definitions of crime.

As differential association, imitation, and definitions take place online, so does differential reinforcement. Reinforcement of behaviors may occur through virtual peers or through peers in person (Holt, 2007; Holt et al., 2010; Higgins 2006). For example, an offender may post threatening or harassing messages online. Virtual peers may comment on the post in a

supporting way that reinforces the behavior. Additionally, in person peers may also praise the offender for the posting. Both forms of differential reinforcement, separately or together, can play a role in reinforcing these behaviors for the offender.

Each of the components of social learning theory may be applied to various types of cyber-crime. Holt et al. (2010), Higgins (2006), Holt and Bossler (2008), Bocij (2004), and Holt (2007) each showed ways in which this theory explains cyber-crime perpetration. This shows that as society develops, this theory may continue to be applied to numerous forms of crime. The theory simply must be adapted to include interactions and relationships that do not take place face-to-face.

Social learning theory most commonly is applied to offenders of crime, but not other actors within the criminal justice system. This theory could be applied to law enforcement officers and prosecutors in order to evaluate how law enforcement officers and prosecutors learn to investigate and prosecute crimes. Law enforcement officers and prosecutors may learn how to adjudicate crimes through the actions of their peers and have their actions reinforced through the successful prosecution of similar cases. While this theory may be applicable for crimes such as cyber stalking, the current study is focused more on the actual actions of law enforcement officers and prosecutors and less on how they learned to take those actions. Additionally, evaluating how law enforcement officers and prosecutors learned to adjudicate crimes would require data directly from the actors.

Another appropriate and common theory to use when explaining criminal behavior, including cyber-crime, is the general theory of crime. The general theory of crime suggests that individuals with low levels of self-control have an increased likelihood of engaging in criminal behavior (Gottfredson & Hirschi, 1990). The studies related to cyber-crime perpetration show

that a relationship exists between low levels of self-control and the perpetration of some forms of cyber-crime such as piracy (Higgins et al., 2007) and cyber stalking (Marcum et al., 2014). It may be possible that individuals with low levels of self-control could be more likely to engage in cyber-crimes due to the desire for instant gratification. The virtual world is all about instant gratification. Cyber stalking, for example, allows someone to stalk the target at a moment's notice. They have the ability to pull up a social media account, send a message, or monitor activity through tracking software without having to leave their current location or know where the victim is currently located. This fulfills the offender's need for instant gratification caused by low self-control. Individuals with low self-control may pirate movies instead of waiting for them to come out on video, send harassing messages without having to wait until they see them, among various other activities. We could also theorize that the environments that allow for broad access, fast responses, and complete anonymity, thereby minimizing the consequences one suffers for inappropriate behavior, self-control would be at an all-time low.

Researchers also applied the general theory of crime to cyber-crime victimizations (Holt & Bossler, 2009; Bossler & Holt, 2010). These studies showed relationships that were not very strong and may not apply to all forms of cyber-crime victimization. Holt and Bossler (2009) found that individuals with low levels of self-control may be more likely to interact with deviant peers, thus making them more likely to interact with potential offenders. In an additional study, Bossler and Holt (2010) found that the impact self-control had on victimization was mediated by the association with deviant peers. The study found that, "individuals with inadequate levels of self-control choose to associate with peers who commit computer deviance, who in turn intentionally or unintentionally victimize their peers" (Bossler & Holt, 2010, p. 233).

Higgins, Fell, and Wilson (2007) and Marcum, Higgins, and Ricketts (2014) showed that the general theory of crime may be applied to cyber-crime perpetration. There appears to be a relationship between low self-control and the perpetration of cyber-crime, due to individuals seeking instant gratification. However, Bossler and Holt (2010) and Holt and Bossler (2009) showed that the general theory of crime does not successfully apply to cyber-crime victimization. Aside from being more likely to interact with deviant peers, having low self-control does not seem to make individuals more likely to be victimized virtually (Holt & Bossler, 2009).

Similarly to social learning theory, the general theory of crime is most commonly applied to offenders of crime. The general theory of crime would not be an effective theory to apply to other criminal justice actors, such as law enforcement officers or prosecutors. In order to apply the general theory of crime to these actors, the assumption would be made that law enforcements officers and prosecutors choose whether or not to adjudicate crimes because of their own levels of self-control.

Another theory, routine activity theory, also has applications for cyber-crime. The routine activity theory suggests that the convergence of likely offenders, suitable targets, and no capable and willing guardians in time and space may lead to criminal activities (Cohen & Felson, 1979). This theory seems to drive the greatest amount of inconsistency when applied to cyber-crime victimization. Yar (2005) argues that the theory may not be applied to cyber-crime because the offenders and victims do not converge in time and space. However, Reyns, Henson, and Fisher (2011) argue that space convergence does take place in cyber space. While the convergence may not occur immediately after the offender commits the crime, eventually the victim and offender converge (Reyns et al., 2011). But another point with stalking is that the convergence in space does not necessarily happen at the same time in face-to-face stalking either. For example, an

offender may leave a note on a victim's car and the victim may not locate the note until a later time. As another example, compare a cyber-crime such as identity theft to a home burglary. In both cases, the target would not be the individual, but the money or the belongings owned by the individual. Both crimes may take place without the victim's knowledge and may take time to be detected. Perhaps the key here is that the convergence in space happens in the face-to-face world, but happens in asynchronous time in the virtual world.

Researchers also disagree about capable guardianship. While Hollis, Felson, and Welsh (2013) argue that guardianship requires a human element, Reyns et al. (2011) and Holt and Bossler (2008) argue that technology may act as a guardian. The type of guardianship necessary, however, may depend on the type of crime. For example, as Holt and Bossler (2008) pointed out, virus protection software may help to prevent identity theft, but would not stop offenders from sending harassing messages. The argument could be made that human guardianship may take place virtually. If an individual is receiving threatening or harassing comments online, another individual may step in and attempt to stop the offender from continuing the harassment. Also, human moderators in groups, chat rooms, and blogs may assist in stopping harassing messages from appearing. On the other hand, virtual tools may also act as guardians. Utilizing anti-virus software, blocking potentially harassing individuals, or not allowing strangers to search for one's profile may stop victimizations. Reyns et al. (2016) found that in person guardians may not be effective. As people can communicate online without other's knowledge, offline guardians may not know that individuals are at risk for victimization.

The concept of target attractiveness, while also different in cyber space, also likely applies to cyber-crimes. In person, targets may appear attractive for crimes due to their appearance, the value of their belongings, or their routines. Online, targets may appear attractive

due to their online availability and how they portray themselves virtually. As Holt and Bossler (2008) point out, the amount of time online does not directly impact the likelihood of cyber-crime victimization. However, the types of activities taking place online do impact victimization (Holt & Bossler, 2008). In particular, utilizing chat rooms and instant messaging services made individuals more likely to be harassed online (Holt & Bossler, 2008). An individual's level of virtual presence and how they are portrayed may make them attractive targets to potential offenders online.

Despite arguments from other researchers, both Reyns et al. (2011) and Holt and Bossler (2008) make compelling arguments that routine activities theory applies to cyber-crime victimization. The components of the theory need to be adapted in order to work with the virtual world, such as using virtual guardians for some crimes and human guardians for others. Just as with social learning theory, routine activities theory will continue to need adaptation as society progresses. As with the general theory of crime, routine activities theory would not be appropriately applied to other criminal justice actors, including law enforcement officers and prosecutors.

Applying social learning theory, the general theory of crime, and routine activities theory requires flexibility and imagination regarding the main ideas of the theories and how they can be applied to a world they were not originally meant to explain. While not initially conceptualized to explain crimes in the virtual world, each of these theories may be applied to cyber-crime by likening the various noteworthy behaviors in which people engage in the real world to corresponding behaviors in the cyber world, As an example, routine activities theory notes that individuals who leave their homes for leisure are more exposed to potential offenders and are therefore more likely to be victimized than those who stay at home. Similarly, it may be that

individuals in the cyber world, who “go out” and interact in a chat group may have a greater risk for victimization than those who are just surfing the web. At the same time, individuals who stay home a lot playing video games may be more likely to be victimized online than if they left the home. So, adapting each of the theories to accommodate the differences between the real world and the virtual world makes them more applicable. The points of the theory remain intact with these corresponding adaptations and despite arguments from researchers they may be able to be applied to cyber-crime and victimization with only a few accommodations.

Even though social learning theory, the general theory of crime, and routine activity theory each have their own strengths and have been used frequently to explain cyber-crime and stalking, they are not the best choice of theory for the present study. As noted, social learning theory is applied most often towards understanding how criminals learn behaviors. In a study such as this one, social learning theory would be most appropriate for attempting to understand how cyber stalkers learn how to increase surveillance, harass victims, and generally use the tools and methods in order to commit offenses. However, as this study focuses on methods used, arrest, and prosecution, this theory would not be the most suitable. Similarly, the general theory of crime focuses on factors that may influence potential criminal behavior. Concepts such as self-control may explain why a cyber-criminal may engage in that behavior, but do not offer much in terms of explaining why an offender may get arrested or prosecuted while another does not. Finally, routine activities theory focuses on factors that increase the likelihood of a crime occurring. In particular, how the behavior of the victim, offender, and potential guardian influences the occurrence of a criminal event. As this study is less interested in why a person stalks and more interested in why one offender was arrested or why one crime was prosecuted over another, this is not the strongest choice.

Since the present study examines the factors influencing the decision making of law enforcement officers and prosecutors, a theory with a focus on decision making, and not on behavior, is better suited. While often seen applied to criminal behavior and crime prevention, the theory to be used in this study, rational choice theory, has very rarely been applied to cyber-crime nor has it been used to explain the actions of other criminal justice actors. Rational choice theory in criminology may be tied back to the classical school of criminology with Cesare Beccaria and Jeremy Bentham. Prior to the classical school, the belief existed that those who committed crimes were possessed by demons and were not in control of their own actions (Fox, 1962; Levack, 1995). Cesare Beccaria shifted those ideals by indicating that individuals have free will and make decisions about whether or not to commit crimes (2009). Beccaria (1764/2009) also stated that individuals base their decisions whether or not to commit crimes on the potential punishments, a concept known as deterrence. Jeremy Bentham (1789/1996) took this a step further and indicated that individuals not only weigh the potential punishments of committing a crime, but also weigh the potential pleasures as well, a concept known as hedonistic calculus. These basic principles lay the foundation for what criminologists now know as rational choice theory.

Rational choice theory in criminology assumes that offenders weigh the costs and benefits of their decisions prior to committing a crime (Cornish & Clarke, 1987). As the name implies, individuals make a calculated analysis in order to determine whether a choice is "rational" (Cornish & Clarke, 1985). In this theory, criminals are not simply "passive figures" with a psychological predisposition towards offending, but active agents who analyze the risks involved (Clarke & Cornish, 1985).

Clarke and Cornish (1985) state that there is a rational choice in every situation, however people may not always follow it due to a variety of factors including life experiences, fears, and prejudices. Impulsivity, self-control, punishment, attachments, and environmental constraints may also play a role in whether individuals make the most rational choice or not (Pratt, 2008). Researchers also suggest that while these factors influence how individuals make decisions, some may be more adept at making the most rational ones due to being better at collecting information (Paternoster & Pagarsky, 2009).

In the rare instances that rational choice theory has been applied to cyber-crime, studies found that the offenders do not believe they will be caught for their crimes (Hutchings & Clayton, 2016). Due to the anonymous nature of cyber space, those engaging in cyber-crimes may believe that their identities will remain hidden and they will never be caught for their crimes. This anonymity may be seen as a major benefit when weighing the costs and benefits of committing cyber-crimes.

Although rational choice theory is predominantly used to explain the decision making of offenders, there is no reason to think it could not be used to explain the behavior of other criminal justice actors such as law enforcement officers, prosecutors, and victims. Just as offenders make rational decisions based on the costs and benefits of committing the crime, others may weigh the costs and benefits of reporting the crime, investigating or cooperating with the investigation of the crime, and/or adjudicating the crime. Indeed, research suggests prosecutors are rationally considering such factors as quality of evidence and level of victim cooperation when making a determination in cases of domestic violence (Westera & Powell, 2015). Research also shows that law enforcement officers also make rational considerations about whether or not to arrest a subject in domestic violence incidents. Research has highlighted such factors as

injunction violations and increased risk of harm to the victim (Kane, 2000). In this study the theory will be used to explain decision making of law enforcement, prosecution, and victims. Rational choice theory is the best theory for this study as both law enforcement officers and prosecutors must weigh the costs and benefits of their decisions to move forward with each case. Law enforcement officers and prosecutors are also limited by a few factors, including time, their own cognitive ability, and the information they have available (Cornish & Clarke, 1987).

Law enforcement officers and prosecutors of cyber stalking cases may also be impacted by what Clarke and Cornish (1985) called "importance beliefs," referring to beliefs that stem from past experiences, fears, and prejudices, when making the rational choice to move forward with cases. When examining importance beliefs, it is possible that law enforcement officers and prosecutors may believe that stalking, whether cyber or face-to-face, is a crime that is not as important as other crimes (Logan & Walker, 2007; Brewster, 2001; Logan & Cole, 2007; Logan et al., 2002; Jordan et al., 2003). In this view, law enforcement officers may not feel that cyber stalking is viewed as important by the community or by prosecutors, and therefore not worth the time and effort necessary to make arrests and/or refer cases to prosecutors. In particular, law enforcement officers may minimize the impact of cyber stalking, as they may not understand how behaviors such as threats on social media can cause fear in victims (Marcum & Higgins, 2019). Cyber stalking may result in psychological harm to victims, but not physical harm that is more obvious to those in the criminal justice system (Finch, 2001; Logan & Walker, 2017; Spitzberg, 2002).

Additionally, prosecutors on these cases may not view cyber stalking as a crime that is as important as others and therefore may not feel prosecuting these cases is worth the necessary time and effort. Prosecutors of cyber stalking cases may feel as though they are putting their jobs

in jeopardy if they lose in court, and therefore do not move forward with the cases they are not confident they can win. Research on prosecutors has shown that some State Attorney's Offices keep "score" of prosecutor's wins and losses and others require prosecutors to file reports on cases they lose (Ferguson-Gilbert, 2001). In offices such as these, promotions are dependent on the "scores" of convictions, leading prosecutors to "become motivated by their own self-interests to win cases rather than their interests in serving the public" (Ferguson-Gilbert, 2001, p. 293). As cyber stalking is a difficult crime to prove, prosecutors may feel as though these cases are not worth the risk. On the other hand, prosecutors may choose to move forward with prosecuting cases of cyber stalking simply to make a point that cyber stalking cases are being taken seriously, either towards the community or specific offenders. Law enforcement officers and prosecutors determine whether the risks are worth the reward.

Rational choice theory may also be applied to the victims of cyber stalking in a number of different ways. Victims make choices throughout their victimizations that impact how their cases are treated within the criminal justice system. Initially, victims choose how they handle the situations prior to reporting to law enforcement. Protective measures including blocking social media accounts, changing phone numbers, obtaining restraining orders, informing friends and family members, shutting down social media accounts altogether, and documenting cyber stalking instances may assist later in the prosecution of these cases. Additionally, victims may weigh the costs and benefits to reporting cyber stalking to law enforcement and may feel their situations are not serious enough to report. Victims of cyber stalking may also feel that law enforcement is not equipped to investigate their cases or prevent future occurrences (al-Khateeb et al., 2016). Once reported, however, victims must also make the choice whether or not to cooperate in the investigative and prosecution processes. Some victims may choose to move

forward with participating and may become upset if offenders are not arrested or if prosecutors choose to drop the cases, while other victims may choose not to cooperate for a variety of reasons such as fear of reprisal. Here, victims may feel as though the risks outweigh the benefits in these cases, especially if they feel as though they may be in danger by participating in the investigation or prosecution process. Throughout cyber stalking situations, victims have to make a number of rational choices that may influence the arrest or prosecution of offenders.

Clearly, this theory is the most appropriate for the current study because it can be applied in multiple ways. First, rational choice theory can apply to law enforcement officers as to why they would choose whether or not to arrest offenders and the choices regarding who law enforcement refers cases to. This theory also applies to the prosecutors as to why they would or would not choose to prosecute cases of cyber stalking. Law enforcement officers and prosecutors may view cyber stalking cases as too risky, not important enough, or the costs may not outweigh the benefits. Additionally, rational choice theory also applies to victims in their decisions as to what, if any, measures to take to prevent future occurrences of cyber stalking by offenders. Theoretically, offenders, prosecutors, and victims make rational choices in cyber stalking cases that are applicable in this study. Making rational choices about criminal behavior after it is committed by those affected and those charged to respond is just as expected as it applies to the behavioral decision making in the first place.

CHAPTER 4: METHODOLOGY

This study examines cyber stalking from a quantitative perspective using rational choice theory for its theoretical underpinning. By extending the theory and applying it to law enforcement officers, prosecutors, and victims, this study assesses rational choice theory as a way to increase our understanding of the factors that influence the progress of face-to-face and cyber stalkers as they progress through (or drop out of) the criminal justice system.

The current study uses quantitative data to address some of the gaps in the current cyber stalking literature. Specifically, from an empirical outlook this study answers two important questions. First, how do the various methods used by offenders of cyber stalking impact their arrest and prosecution decisions? Second, how do victims' actions impact arrest and prosecution decisions in cases where they have been victims of cyber stalking? The study also evaluates demographic characteristics and their influence over law enforcement and prosecutorial actions. Finally, this study provides a description of face-to-face and cyber stalking tools and techniques. This provides some evidence for the on-going debate of whether cyber stalkers are a unique type of criminal, or if they are the same old stalkers with new gadgets and technology.

The results of this study will show how law enforcement officers and prosecutors look at cyber stalking cases. If the methods used by offenders of cyber stalking have no significant impact on arrests or prosecution, then we can infer that these are not elements that law enforcement officers and prosecutors take into account when making choices about whether or not to move forward with cases. However, if these factors do have a statistical impact, then we know that law enforcement officers and prosecutors do take them into consideration when deciding whether to arrest or prosecute offenders of cyber stalking. This has strong implications

for rational choice theory and whether it is a viable perspective for understanding the factors that influence the progress of stalkers through the criminal justice system.

Similarly, the results will highlight whether law enforcement officers and prosecutors who interact with victims are influenced by these victims' actions when making their own arrest and adjudication decisions. For example, if we find that cases in which victims were proactive, including actions such as whether the victim obtained an order of protection or blocked the offender on social media were handled differently by law enforcement officers and prosecutors then we know that victims can have influence over the processing of their cases.

Data

For this study, the data are all stalking cases reported to law enforcement between the years 2015-2017, in the Central Florida counties of Orange, Brevard, and Seminole. The unit of analysis is the stalking case. The Sheriff's Offices in these counties do not indicate they have specialized stalking units or officers specifically trained to investigate stalking cases.

Data Collection

The state of Florida was chosen for this study due to the open public records law. Florida Statute 119.01 states "It is the policy of this state that all state, county, and municipal records are open for personal inspection and copying by any person." Public records requests were made for all law enforcement reports that fell under Florida Statute 784.048 for the Sheriff's Offices in Orange, Brevard, and Seminole counties from 2015 to 2017. These counties make up the core of the Central Florida region. The year range was chosen in order to ensure the majority of cases

would have had a chance to be fully processed by the judicial system, thereby making certain that a sufficient number of reports could be evaluated for quantitative analyses. A total of 888 reports were collected, reviewed, and tracked (Orange County: 525; Brevard County: 131; Seminole County: 232). Of the 888 reports reviewed and tracked, 884 were able to be tracked to their conclusion.

The law enforcement reports were meticulously reviewed and coded, with forty-five variables being collected, coded, and tracked. The variables collected included information regarding the victim and offender demographics, the methods utilized by the offender, the actions taken by law enforcement, and the actions taken by prosecutors. The law enforcement reports included the date, time, and location of the report, demographic and personal information regarding the offender and victim, such as name, address, date of birth or age, race, ethnicity, gender, driver's license number, and physical description, and the potential charges associated with the reported behavior. The reports also included narrative sections that involved written descriptions from the law enforcements officers about their interactions with the victims, the information reported by the victims, and the steps taken immediately following the collection of information. The narrative sections included information from victims regarding the tactics used by the offenders, and the tactics were tracked based on this information. In some cases, the reports did not include complete information about the offenders or victims, either for confidentiality purposes or if the information was unknown. Additionally, some of the cases did not include information regarding the offender and victim relationships or the actions taken by law enforcement officers following the report. In these events, these variables were coded as missing.

In addition to the law enforcement reports, the names of the offenders were also searched in the records of the corresponding Clerk of Court in order to track charges, trials, and verdicts. Some of the offender names were redacted in the police reports, however, the majority of missing offender names were able to be located by searching for injunctions filed by the victims. In order to locate these offender's names, the victim's names, if listed, were searched in the Clerk of Court records and often resulted in injunctions filed around the same timeframe as the police report that listed the names of the offenders.

The State of Florida defines stalking as, "willfully, maliciously, and repeatedly" following, harassing, or cyber stalking another person (FLA STAT. ANN. § 784.048). Cyber stalking in Florida, listed within the stalking statute, is defined as, "to engage in a course of conduct to communicate, or to cause to be communicated, words, images, or language by or through the use of electronic mail or electronic communication, directed at a specific person" (FLA STAT. ANN. § 784.048). While not listed in Florida's stalking statute, another Florida statute defines electronic communication as, "any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic, or photoopical system" (FLA STAT. ANN. § 934.02). As Florida does not have separate statutes for stalking and cyber stalking, but lists cyber stalking directly under the stalking statute, I am unable to determine which stalking tactics would be viewed by law enforcement officers or prosecutors as face-to-face or cyber tactics. As a result, I chose to include all forms of electronic communication, including communication by phone, text message, e-mail, and social media as cyber tactics.

In addition, at the time of this study, Florida's statute on sexual cyber harassment, sometimes known as "revenge porn," only included sexually explicit images that were published

on websites without the permission of the victims (FLA STAT. ANN. § 784.049). Some of the cases in this study involved sexually explicit images that were shared via e-mail, text message, or social media. As a result of the limitations of this statute, these cases were often categorized by law enforcement as stalking. However, in 2019 a new bill passed in Florida expanding the sexual cyber harassment statute to include images shared through electronic means beyond just websites (Cyberharassment, CS/HB 1043, 2019). Therefore, the current study includes cases classified as stalking that may not have been classified as stalking if the statute updates were in place.

Confidentiality

The names and identifying information of the victims were not tracked in order to protect the confidentiality of the victims. In addition, some of the names and demographics of the victims were not available due to confidentiality laws. Again, in these cases, this information was coded as missing.

Measures

Dependent Variables

The dependent variables in this study are whether or not the offender in each case was arrested or had charges filed, taken to trial, and/or found guilty. The arrest variable measures whether there was an arrest by law enforcement that was documented within the police report or if there was a Notice to Appear provided to the offender indicating that initial charges had been filed through the State Attorney's Office. Cases with an arrest or charge were coded as 1 and those without an arrest or charge were coded as 0. Cases were coded as 1 if there was an arrest

made or charges filed in any of the cases reviewed, regardless of whether the prosecutors changed the charges to something other than stalking. The trial variable measures whether the prosecutors assigned to the case continued with it or dropped the charges at any point after the offender had been charged with the crime. Cases in which the offender plead guilty were coded as 0 and the plea was tracked separately and not evaluated in this study. The trial variable was only recorded in cases in which the arrest variable was 1. Cases in which a judge or jury determined the final verdict were coded as 1 and those in which the prosecutors filed No Information Reports or declined to prosecute were coded as 0. The guilty verdict variable measures whether cases that went to a judge or jury resulted in a guilty verdict. This variable includes cases in which the judge made the final decision through a bench trial and cases in which a full jury trial took place. The guilty verdict variable was only recorded in cases in which both the arrest and trial variables were 1. Cases with a final verdict of guilty were coded 1 and those with a not guilty verdict were coded 0.

Independent Variables

Independent variables in this study include mode of stalking (cyber, face-to-face, or combination), various cyber tactics used including phone call, text message, e-mail, social networking, video/photo, tracking device, doxing, as well as direct threats, total number of tactics used, victim and offender relationship, and victim action. The law enforcement reports did not include a checklist of the independent variables tracked, but required interpretation by the researcher in order to track the modes and tactics used. Additionally, some of the independent variables in this study measure the mode of stalking and some of variables measure the various

tactics used. The mode variable measures whether the stalking in each case was done electronically (cyber), face-to-face, or through a combination of both. The mode variable was coded as 1 for cyber, 2 for in person, and 3 for both.

The phone call, text message, e-mail, and social networking variables measure whether offenders in each cases utilized these electronic means to communicate with the victims. These variables were each coded at 1 for yes and 0 for no. The video/photo variable measures whether the offender in the cases publicly shared a photograph or video of the victim without their knowledge or consent, and was coded as 1 for yes and 0 for no. The tracking device variable measures whether the offender in each case installed a tracking device on the victim's cellular phone or vehicle in order to track the victim's location and was coded as 1 for yes and 0 for no. The doxing variable measures whether offender in the cases publicly shared any personal information of the victim, including contact information and location information, and was coded as 1 for yes and 0 for no. The direct threats variable measures whether the offenders in the cases made direct threats of harm, either face-to-face or electronically, to the victim and was coded as 1 for yes and 0 for no. The total tactics variable measures the number of tactics used by the offender in each case and includes a total sum from variables direct threats, phone call, text message, e-mail, tracking device, social networking, doxing, and video/photo. The total tactics variable is numerical and ranges from 0 to 8.

Independent variables in this study also measure the relationship between the victim and offender and the actions taken by the victim to abate the offender's behaviors. The victim and offender relationship variable measures the type of relationship between the victim and offender and includes partner (1), spouse (2), family member (3), coworker (4), neighbor (5), ex of partner or partner of ex (6), acquaintance (7), stranger (8), or unknown (9). The victim action variable

measures whether the victim was proactive in their efforts to prevent the behaviors from continuing. For this study, I identified three proactive actions, including the victim telling the offender to stop the behavior, blocking the offender electronically, or obtaining or attempting to obtain an injunction for protection. The reports did not include any additional proactive behaviors by the victims. The victim action variable was coded as 1 if the victim engaged in any of the possible proactive behaviors and 0 if the victim engaged in none of the proactive behaviors.

Control Variables

Demographic control variables were also included in this study. The race, ethnicity, gender, and age of both the victim and offender were tracked; however, ethnicity, limited in the reports to "Hispanic" or "Non-Hispanic," was not utilized due to the majority of police reports missing the data. The offenders' race and victims' race variables included White (1), Black (2), Asian (3), Pacific Islander (4), American Indian (5), other (6), unknown (7), and missing (8). An examination of these variable's frequencies showed that 98.7% of the sample for offenders and 98.9% of the sample for victims were White, Black, unknown, or missing, so these variables were recoded to 0 for White and 1 for Black, with all others being coded as missing. The offender gender and victim gender variables included Male (1), Female (2), other (3), unknown (4), and missing (5). An examination of these variable's frequencies showed that no offenders or victims were categorized as other, therefore the offender gender and victim gender variables were recoded to 0 for Male and 1 for Female, with all others being coded as missing. The offender age and victim age variables were continuous and included numerical values between

the range of 13 to 85. The offender age and victim age variables were also recoded into separate variables as Under 18 (1), 18-24 (2), 25-34 (3), 35-44 (4), 45-54 (5), and 55 and Over (6).

Analytic Strategy

Analyses of the variables were conducted at the univariate, bivariate, and multivariate levels. Frequency distributions and measures of central tendency were measured for the independent variables and dependent variables. Chi-square tests were used in order to examine the relationship between the independent variables and dependent variables on the bivariate level. Additionally, chi-square tests looking at the relationship between various independent variables and dependent variables (i.e., the model) were completed after selecting cases based on mode used, including only cyber cases and combination cases. Logistic regression models were used to predict the odds of arrest depending on various independent variables. As only 213 cases moved beyond an arrest or charges being filed, and only 81 cases proceeded through a full trial, there were not enough cases to run logistic regression models for these dependent variables.

Unique Cases

While this study is quantitative, there were some cases that stood out as being unique and are worthy of discussion. As stated in the Cyber Stalking Methods & Tools section, offenders of stalking occasionally utilize spoofing applications or tracking software on their victims. Several reports indicated that victims received phone calls from a variety of phone numbers. Many of the victims reported answering the phone calls and finding their offenders on the other side. While not confirmed in the reports, it appears as though the offenders may have been using spoofing

applications to make phone calls appear as though they are coming from different phone numbers. One victim reported utilizing a prevention strategy discussed in the Cyber Stalking Prevention Strategies section. This strategy involved the victim using a phone application called Trapcall in order to unblock the phone number of a blocked call. The application showed that the caller in this situation was the offender. Another victim took her cellular phone to her carrier, and was informed by the carrier that a tracking application had been installed on her phone remotely. The offender in this situation did not have physical access to the phone to install the tracking software, however, the software had been installed and ran continuously and sent location data to the offender.

In addition to the tracked data being used in this study, I also tracked the number of charges filed against the offenders in the cases beyond the initial charges of stalking. In the cases that included other charges, the vast majority included only one or two. However, one case involved an offender contacting a victim while there was an injunction for protection in place. The prosecutors in this case charged the offender with Violation of Injunction for protection for every phone call, text message, and e-mail sent, resulting in a total of 326 additional charges beyond the stalking charge. Until this case, the highest number of charges filed against one of the offenders was eight.

In addition, I found a number of cases that involved direct threats of harm to the victims, including some offenders that sent images of guns to provoke fear in their victims, yet no arrest was made or charges were filed. Conversely, there were other cases that did not appear to cause fear or significant emotional distress, such as an offender posting a singular negative review on the business Facebook page of a victim, or an offender placing dog excrement in a neighbor's

driveway on three occasions, but these cases resulted in not only charges being filed, but guilty verdicts. These cases show the complexity of factors that impact outcome decisions.

CHAPTER 5: RESULTS

The current study answers the questions: how do the various methods used by offenders of cyber and face-to-face stalking impact arrest and prosecution action and how do the victim's actions impact arrest and prosecution actions in stalking cases? The study also evaluates demographic characteristics and their influence over law enforcement and prosecutorial decisions. This chapter begins with univariate description of the dependent variables, independent variables, and control variables. The univariate analyses provides information regarding the demographic characteristics of offenders and victims, tactics utilized by offenders of cyber stalking, relationships between offenders and victims, and the actions taken by victims. In addition, univariate analyses provides the outcomes of stalking cases. The chapter then discusses bivariate analyses that examine the relationships between the independent variables and dependent variables. These analyses show which of the independent variables impact dependent variables, in particular, which independent variables impact arrest decisions. Finally, this chapter closes with a discussion of the multivariate analyses that show the odds of arrest based on numerous independent variables.

Univariate Analysis

Frequency distributions for the demographic characteristic of offenders and victims in the stalking offenses reported to law enforcement are presented in Table 1. These tell the descriptive story of the actors involved in the present cases under analysis. The race for offenders was reported as 72.2% white and 27.8% black and the race for victims was reported as 81.4% white and 18.6% black. The majority of offenders were male (80.8%), with not quite 1/5th being female

(19.2%), while the majority of victims were female (81.3%), with only 18.7% being male. The ages reported for offenders ranged from 15 to 85 and for the ages reported for victims ranged from 13 to 75. The mean age for offenders was 36.9 and the mean age for victims was 34.8. This univariate analysis shows that the offenders in these cases are young to middle aged white males who are stalking slightly younger white females.

Table 1 Demographic Characteristics of Stalking Offenders and Victims by Mode

	Cyber Cases	Face-to-Face Cases	Combination Cases	Total
	%	%	%	%
Offender Race	(N=260)	(N=143)	(N=339)	(N=742)
White	79.2	67.8	68.7	72.2
Black	20.8	13.1	31.4	27.8
	%	%	%	%
Offender Gender	(N=271)	(N=146)	(N=350)	(N=767)
Male	78.2	79.5	83.4	80.8
Female	21.8	20.5	16.6	19.2
	Mean	Mean	Mean	Mean
Offender Age	(N=256)	(N=138)	(N=331)	(N=725)
	36.2	41.3	35.6	36.9
	%	%	%	%
Victim Race	(N=291)	(N=157)	(N=322)	(N=770)
White	87.3	80.9	76.4	81.4
Black	12.7	19.1	23.6	18.6
	%	%	%	%
Victim Gender	(N=299)	(N=158)	(N=329)	(N=786)
Male	20.1	19.0	17.3	18.7
Female	79.9	81.0	82.7	81.3
	Mean	Mean	Mean	Mean
Victim Age	(N=210)	(N=117)	(N=234)	(N=561)
	35.2	36.5	33.7	34.8

Table 2 presents the frequency distributions for the mode of stalking variable utilized in this study. Based on the review of the law enforcement reports, 38.1% of the cases included cyber, or electronic, tactics alone while 19.8% of the cases included face-to-face tactics alone. This leaves 42.1% of cases that involved both cyber and face-to-face tactics. This provides some

initial information that can speak to the debate of whether cyber stalking is a new crime or an extension of traditional face-to-face stalking. We can infer from these frequencies that the majority of stalkers who utilize face-to-face tactics also incorporate cyber tactics.

Table 2 Mode of Stalking

		%
Mode		(N=888)
	Cyber Only	38.1
	Face-to-Face Only	19.8
	Both Cyber and Face-to-Face	42.1

Table 3 presents the frequency distributions for the mode of stalking by county. The reports indicate that Orange County, the largest county in the Central Florida area, with 525 reports of stalking between 2015 and 2017, had a majority of cases with both cyber and face-to-face components. Seminole County, with 232 reports of stalking, had an almost equal number of cyber cases and combination cases during the timeframe reviewed. Brevard County, with 131 reports of stalking, showed over half of stalking cases were cyber in nature.

Table 3 Mode of Stalking by County

		Cyber Cases %	Face-to-Face Cases %	Combination Cases %
Orange	N=525	33.0	21.9	45.1
Seminole	N=232	40.5	18.5	40.9
Brevard	N=131	54.2	13.7	32.1

Table 4 shows the frequency distributions for the tactics used by stalking offenders in these cases by the mode used. The reports indicate that in all cases, 46.7% of offenders made phone calls to victims and 53.3% did not. In cyber cases, 48.5% of offenders made phone calls and in combination cases 67.1% of offenders called the victims. The reports also show that 50.7% of offenders in all cases sent text messages to victims and 49.3% did not. For cyber cases, 58.0% of offenders used text messages, while for combination cases 67.9% of offenders sent text messages. Phone calls and text messages were used more frequently in cases that involved both cyber and face-to-face tactics than in those cases with cyber tactics alone.

According to the reports, only 13.0% of all cases involve e-mail, while 87.0% do not. In the cases reviewed, 17.8% and 14.7% include e-mails in cyber and combination cases respectively. The reports also indicate that 30.7% of all cases involve social networking sites and 69.3% do not. In cyber cases, 48.5% of offenders used social networking, and 29.1% of offenders used social networking in combination cases. Much like e-mail, social networking was used more frequently in cyber cases than in combination cases. Also, the reports show that offenders posted a video of a photograph of victims without their consent in 8.8% of all cases, but did not in 91.2% of cases. In cyber cases, 17.5% of offenders posted a video or photo, while in combination cases 5.1% posted a photo or video. So, e-mail, social networking, and photographs or videos were used more frequently in cyber cases than in cases involving both cyber and face-to-face tactics.

Additionally, the reports show that 96.8% of offenders did not utilize a tracking device while 3.2% did. For cyber cases, the percentage of cases involving tracking devices was 2.1%, while the percentage for combination cases was 5.6%. Offenders using a combination of cyber

and face-to-face tactics used tracking devices more frequently than offenders using only cyber tactics.

The reports also indicate that in all cases 95.6% of offenders did not dox or publicly share personal information about their victims while 4.4% did. However, in cyber cases 9.2% of offenders were reported as doxing their victims compared to 2.1% for combination cases. Cases involving cyber tactics involved doxing more frequently than cases involving a combination of cyber and face-to-face tactics.

The total number of tactics were also calculated, and the number of tactics used ranged from 0 to 6, although the highest possible total was 8. The mean for the total tactics used by offenders was 1.58.

Table 4 Tactics Used by Offenders of Stalking by Mode

	Cyber Cases % (N=338)	Combination Cases % (N=374)	Total % (N=888)
Phone Call			
Yes	48.5	67.1	46.7
No	51.5	32.9	53.3
Text Message			
Yes	58.0	67.9	50.7
No	42.0	32.1	49.3
E-Mail			
Yes	17.8	14.7	13.0
No	82.2	85.3	87.0
Social Networking			
Yes	48.5	29.1	30.7
No	51.5	70.9	69.3
Video/Photo			
Yes	17.5	5.1	8.8
No	82.5	94.9	91.2
Tracking Device			
Yes	2.1	5.6	3.2
No	97.9	94.4	96.8
Doxing			
Yes	9.2	2.1	4.4
No	90.8	97.9	95.6
Total Tactics			
0	N/A	N/A	19.9
1	39.3	37.5	30.6
2	34.3	40.6	30.2
3	14.8	15.8	12.3
4	8.9	4.8	5.4
5	2.4	1.3	1.5
6	0.3	0.0	0.1

Table 4 shows that offenders of stalking in cases that included both cyber tactics and face-to-face tactics utilized phone calls, text messages, and tracking devices more than offenders in cases that only involved cyber tactics. Additionally, offenders of stalking in cases that involve only cyber tactics used e-mail, social networking, and shared videos or photo more than offenders in cases that included both cyber and face-to-face tactics. A potential explanation may be that offenders who intend on incorporating face-to-face tactics may use tracking devices to determine the location of victims and prefer communicating directly with victims via phone or text. Conversely, e-mail and social networking, potentially seen as more impersonal than phone calls or text messages, may be preferred by offenders who choose not to engage with victims face-to-face. Additionally, the sharing of video or photo allows offenders to cause distress to victims without making direct contact electronically or face-to-face.

Table 5 shows the percentage of cases that involve a direct threat by the offender. In the reports, a total of 30.6% included information that showed a direct threat of harm by the offender against the victim, while 69.4% indicated direct threats were not made. The frequency distributions for the use of direct threats when looking at the various methods show that 33.7% of cyber cases, 13.1% of face-to-face cases, and 36.1% of combination cases involved direct threats to the victim.

Table 5 Direct Threats by Offenders of Stalking by Mode

	Cyber Cases % (N=338)	Face-to-Face Cases % (N=176)	Combination Cases % (N=374)	Total % (N=888)
Direct Threats				
Yes	33.7	13.1	36.1	30.6
No	66.3	86.9	63.9	69.4

Table 5 also indicates that offenders in cases that involved cyber tactics or a combination of cyber and face-to-face tactics had higher rates of directly threatening victims than those cases that involve only face-to-face tactics. These results imply that the cyber tactics may allow offenders to feel more empowered to send threatening messages towards victims from a distance, as opposed to threatening victims face-to-face.

Table 6 provides the frequency distributions for the relationship between the offender and the victim in the reported cases. The relationships reported included spouse (11.2%), partner (39.5%), family member (2.0%), coworker (4.2%), neighbor (4.0%), ex of partner or partner of ex (4.8%), acquaintance or friend (15.8%), stranger (10.3%), and unknown (8.3%). The frequency distribution for spouse was 8.3% for cyber cases, 9.6% for face-to-face cases, and 14.5% for combination cases. The percentages of cases involving partners were 36.4% for cyber cases, 22.2% for face-to-face cases, and 50.1% for combination cases. Both spouses and partners had the highest frequencies in combination cases than cyber cases or face-to-face cases.

The reports also show that family members were the offenders in 3.4% of cyber cases, 1.2% of face-to-face cases, and 1.1% of combination cases while coworkers were the offenders in 3.4% of cyber cases, 6.0% of face-to-face cases, and 4.1% of combination cases. Neighbors were reported as being the offenders in 1.2% of cyber cases, 16.2% of face-to-face cases, and 0.8% of combination cases. Family members had the highest frequencies in cyber cases, while coworkers and neighbors had the highest frequencies in face-to-face cases.

The percentages of reports involving either the exes of partners or the partners of exes were 5.6% for cyber cases, 0.6% for face-to-face cases, and 6.0% for combination cases. Acquaintances or friends were reported as being the offenders in 20.4% of cyber cases, 10.8% of face-to-face cases, and 14.0% of combination cases. The reports show that strangers were the

offenders in 9.0% of cyber cases, 22.2% of face-to-face cases, and 6.0% of combination cases. Exes of partners or partners of exes had the highest frequencies in combination cases, with cyber cases not far behind. Acquaintances or friends had the highest frequencies in cyber cases, while strangers had the highest frequencies in face-to-face cases. Additionally, the reports include relationships that were unknown due to the identity of the offenders being unknown in 12.3% of cyber cases, 11.4% of face-to-face cases, and 3.3% of combination cases.

Table 6 Relationship between Offender and Victim in Stalking Cases by Mode

	Cyber Cases % (N=324)	Face-to-Face Cases % (N=167)	Combination Cases % (N=365)	Total % (N=856)
Relationship				
Spouse	8.3	9.6	14.5	11.2
Partner	36.4	22.2	50.1	39.5
Family Member	3.4	1.2	1.1	2.0
Coworker	3.4	6.0	4.1	4.2
Neighbor	1.2	16.2	0.8	4.0
Ex of Partner/ Partner of Ex	5.6	0.6	6.0	4.8
Acquaintance or Friend	20.4	10.8	14.0	15.8
Stranger	9.0	22.2	6.0	10.3
Unknown	12.3	11.4	3.3	8.3

The information in Table 6 shows that in all cases, regardless of mode, the most frequent relationship seen between the victim and offender is that they are partners. The second most frequent relationships, however, were acquaintance or friend for cyber cases, stranger for face-to-face cases, and spouse for combination cases. The results suggest that acquaintances or friends may prefer the distance afforded by cyber tactics, while spouses may use a combination of tactics

due to potential physical proximity and/or the need for continued communication. Additionally, strangers may choose victims they see in person and do not have enough personal information to locate virtually.

Table 7 presents the frequency distribution for the victim action variable in this study by the mode used. Overall, victims were reported as being proactive in 52.9% of all cases. When examining the victim's actions by the mode used, victims were reported as taking proactive measures in 52.7% of cyber cases, 35.8% of face-to-face cases, and 61.2% of combination cases.

Table 7 Victim Action in Response to Stalking Offenses by Mode

	Cyber Cases % (N=338)	Face-to-Face Cases % (N=176)	Combination Cases % (N=374)	Total % (N=888)
Victim Action				
Yes	52.7	35.8	61.2	52.9
No	47.3	64.2	38.8	47.1

Table 7 shows that victims in these cases took action to stop the stalking behaviors more often in cyber cases and combination cases than in face-to-face cases. The reasoning behind this may be that action by the victim in cyber or combination cases can be through less personal means, such as blocking a phone number or social media account or sending a text message informing the offender to cease the behavior. Alternatively, victims of face-to-face stalking may be less likely to take action against their offender because they may not want to confront the offender directly or see them in court when they seek an injunction.

Table 8 shows the frequency distributions for the outcomes of cases by mode. The outcomes examined include arrest, trial, and guilty verdict. In total, 24.0% of reports resulted in

an arrest or charges being filed against the offender. Of those that included arrest or charges, 38.0% of the cases went to trial. Additionally, of the cases that went to trial, 92.5% of them resulted in guilty verdicts. Reports of stalking resulted in arrest or charges filed in 14.6% of cyber cases, 28.7% of face-to-face cases, and 30.2% of combination cases. The cases that resulted in arrest or charges being filed resulted in 55.1% of cyber cases, 35.3% of face-to-face cases, and 31.9% of combination cases moving forward to trial. Of the cases that went to trial, 100.0% of cyber cases, 88.9% of face-to-face cases, and 88.6% of combination cases resulted in a guilty verdict.

Table 8 Outcomes of Reported Stalking Offenses by Mode

	Cyber Cases %	Face-to-Face Cases %	Combination Cases %	Total %
Arrest	(N=336)	(N=174)	(N=374)	(N=884)
Yes	14.6	28.7	30.2	24.0
No	85.4	71.3	69.8	76.0
Trial	(N=49)	(N=51)	(N=113)	(N=213)
Yes	55.1	35.3	31.9	38.0
No	44.9	64.7	68.1	62.0
Guilty Verdict	(N=27)	(N=18)	(N=35)	(N=80)
Yes	100.0	88.9	88.6	92.5
No	0.0	11.1	11.4	7.5

Table 8 shows that cases involving only cyber tactics had the least frequent instances of offender arrest or charges being filed. Conversely, cases with cyber tactics had the highest rates of cases going to trial and resulting in guilty verdicts. However, given the small frequency of

cyber cases proceeding to trial, these results may show that law enforcement officers and prosecutors only pursue cyber cases in which they feel certain they will win.

The typical cyber stalker was a white male, mid 30's, who preferred text messages and refrained from making direct threats, while the victim of cyber stalking was primarily a white female, mid 30's, who was the partner of the offender and took some action to stop the behavior. The most common offender of face-to-face stalking was a white male, early 40's, who also did not make direct threats, and the victim was often a white female, mid 30's, a spouse or stranger of the offender and did not take action to prevent the behavior. The combination stalker, using both cyber and face-to-face tactics, was primarily a white male, mid 30's, who preferred phone calls and text messages and refrained from making direct threats, and the victim was often a white female, early 30's, who was the partner of the offender and took action to stop the behavior from continuing.

Bivariate Analysis

Bivariate analyses utilizing each of the independent variables and dependent variables in this study were conducted in order to begin to examine each independent variable's relationship with the dependent variables. In addition, a bivariate analysis was conducted between the county and the outcomes of cases in order to evaluate how the counties pursue stalking cases. Table 9 provides the outcomes of cases by county and shows that Brevard County had the highest rates of arrest, trial, and guilty verdicts over the other two counties. The arrest and trial rates in Brevard County were significantly higher than Orange and Seminole counties. Additionally, while not significant, the rate of guilty verdicts in Brevard County was 100.0%.

Table 9 Outcomes of Reported Stalking Offenses by County

	Arrest %	Trial %	Guilty %
Orange	21.0***	28.2***	90.0
Seminole	21.6***	39.2***	85.0
Brevard	40.9***	57.7***	100.0

* = p < .05, ** = p < .01, *** = p < .001

Table 10 provides the outcomes of reported stalking offenses by the tactics used. According to the bivariate analyses, the phone call, social networking, doxing, and total tactics variables had significant relationships with arrest. Offenders in these cases that utilized phone calls had arrest rates of 27.8% and cases involving social networking had arrest rates of 16.6%. Additionally, offenders who doxed their victims had arrest rates of 10.5%. The arrest rates for the total number of methods used by offenders were 28.6% for 0, 20.2% for 1, 28.1% for 2, 17.4% for 3, 19.1% for 4, 23.1% for 5, and 100.0% for 6.

While the rest of the tactics did not have significant relationships with the outcome variables, there were some additional notable patterns. Of the offenders who used phone calls who were arrested, 43.5% proceeded to trial, and of those that went to trial, 96.0% were found guilty. Offenders in these cases who sent text messages had arrest rates of 23.4%. Those who were arrested and sent text messages had trial rates of 37.1% and of those that proceeded through trial, 92.1% received guilty verdicts. The results show that offenders in these cases who used e-mail were arrested in 20.9% of the cases, and from those arrested, 50.0% went to trial. The cases involving e-mail that went to trial had guilty verdicts in 100.0% of cases. According to the results, for those arrested in cases involving social networking, 40.0% went to trial, and of those that went to trial, 83.3% received guilty verdicts.

Also, in cases where the offender shared a video or photo of the victim, the cases showed offenders were arrested in 22.1% of the cases. In the cases when offenders were arrested and shared a video or photo, 47.1% of the cases proceeded to trial, and of the cases that went to trial, 100.0% had guilty verdicts. The results also show that offenders who utilized a tracking device had arrest rates of 32.1%. For those who were arrested and used a tracking device, 22.2% of the cases went to trial. Additionally, offenders who used a tracking device and whose cases went to trial had 100.0% guilty verdicts. Of the offenders who doxed their victims and were arrested, 50.0% went to trial, and for the offenders who doxed their victims and went to trial, 100.0% received guilty verdicts. For offenders who were arrested, the trial rates for the total number of methods were 35.3% for 0, 36.4% for 1, 37.3% for 2, 47.4% for 3, 33.3% for 4, 66.7% for 5, and 100.0% for 6. Additionally, for those whose cases went to trial, the rates of guilty verdicts were 88.9% for 0, 95.0% for 1, 92.6% for 2, 88.9% for 3, and 100.0% for 4, 5, and 6.

Table 10 Outcomes of Reported Stalking Offenses by Tactics

	Arrest % (N=884)	Trial % (N=213)	Guilty % (N=80)
Phone Call			
Yes	27.8**	43.5	96.0
No	20.6	31.6	86.7
Text Message			
Yes	23.4	37.1	92.1
No	24.6	38.9	92.9
E-Mail			
Yes	20.9	50.0	100.0
No	24.4	36.5	91.2
Social Networking			
Yes	16.6***	40.0	83.3
No	27.2	37.5	95.2
Video/Photo			
Yes	22.1	47.1	100.0
No	24.2	37.2	91.7
Tracking Device			
Yes	32.1	22.2	100.0
No	23.7	38.7	92.4
Doxing			
Yes	10.5*	50.0	100.0
No	24.6	37.8	92.3
Total Tactics			
0	28.6*	35.3	88.9
1	20.2*	36.4	95.0
2	28.1*	37.3	92.6
3	17.4*	47.4	88.9
4	19.1*	33.3	100.0
5	23.1*	66.7	100.0
6	100.0*	100.0	100.0

* = $p < .05$, ** = $p < .01$, *** = $p < .001$

The information in Table 10 suggests that if prosecutors are looking to take winnable cases to trial, they have been successful at making these assessments. In particular, cases involving e-mail, video or photo, tracking devices, or doxing all received 100.0% guilty verdicts when they went to trial. This implies that prosecutors only proceeded to trial with the cases they could win.

Table 11 provides the outcomes of reported stalking offenses by those involving direct threats and those in which victims took action to stop the stalking behavior. The frequencies show that of the cases reported, offenders who made direct threats towards their victims had arrest rates of 30.3%. Of those arrested who made direct threats, 40.2% went to trial, and of those who went to trial and made direct threats, 90.9% received a guilty verdict. Additionally, in the cases in which victims took action, offenders were arrested in 30.6% of cases. From the cases with victim action that resulted in arrest, 36.6% proceeded to trial, and of those that proceeded to trial, 92.3% of cases resulted in a guilty verdict.

Table 11 Outcomes of Reported Stalking Offenses by Direct Threats and Victim Action

	Arrest % (N=884)	Trial % (N=213)	Guilty % (N=80)
Direct Threats			
Yes	30.3**	40.2	90.9
No	21.2	36.6	93.6
Victim Action			
Yes	30.6***	36.6	92.3
No	16.4	41.2	92.9

* = p < .05, ** = p < .01, *** = p < .001

Based off the information provided in Table 11, the only significant differences were found in cases involving direct threats and victim action. Here, those stalkers who made direct threats and those with victims who took proactive action had higher rates of arrest than those that did not. Also interesting, but not significant, is that in the cases that proceeded to trial, cases involving direct threats had higher trial rates, but cases involving victim action had lower trial rates. Additionally, once the cases proceeded to trial, both cases involving direct threats or victim action had lower rates of guilty verdict than those that did not involve direct threats or victim action. These results show that law enforcement officers may take direct threats or victim action into account in their decision making process more often than prosecutors.

Table 12 provides the distributions of cyber tactic usage by offender demographics, including race, gender, and age. According to the cases reviewed, the race of the offender was significant in phone calls, e-mails, social networking, doxing, and direct threats. The cases showed phone calls, tracking devices, and direct threats were involved in cases with black offenders more than those with white offenders. Conversely, text messages, e-mails, social networking, videos/photos, and doxing were used more often in cases with white offenders than those with black offenders.

In the cases reviewed, the offender gender was significant in phone calls and social networking. The cases also show that male offenders used phone calls, text messages, videos/photos, and direct threats more often than cases with female offenders. However, in these cases, female offenders used e-mails, social networking, tracking devices, and doxing more than male offenders.

Upon examining offender age, age was significant in phone calls, text messages, e-mails, social networking, tracking devices, and direct threats. The cases show that offenders between

the ages of 35 and 44 used phone calls more often than the other age groups. Also, in these cases, offenders between the ages of 25 and 34 utilized text messages and made direct threats more often than the other age groups. The cases also show that offenders under the age of 18 used social networking more frequently than the other age groups. Additionally, both offenders under the age of 18 and those between the ages of 18 and 24 utilized videos/photos more than the other age groups, and the offenders between the ages of 18 and 24 doxed victims more than the other age groups. Also, in these cases, offenders between the ages of 45 and 54 utilized e-mail more than the other age groups, while offenders between the ages of 35 and 44 used tracking devices more than the other age groups.

Table 12 Tactics Utilized by Stalking Offenders by Offender Demographics

	Phone Call %	Text Message %	E-Mail %	Social Networking %	Video/ Photo %	Tracking Device %	Doxing %	Direct Threats %
Offender Race								
White (N=536)	46.8*	53.5	16.2*	32.1***	9.5	3.2	5.2*	27.8***
Black (N=206)	55.8*	49.0	6.3*	20.4***	6.3	3.9	1.9*	40.3***
Offender Gender								
Male (N=620)	51.1*	52.7	13.5	26.1***	8.5	3.2	3.5	31.8
Female (N=147)	41.5*	51.0	14.3	42.2***	8.2	4.1	6.8	29.9
Offender Age	***	***	**	***		*		**
Under 18 (N=8)	12.5	50.0	0.0	62.5	12.5	0.0	0.0	37.5
18-24 (N=104)	41.3	53.8	5.8	43.3	12.5	1.0	8.7	36.5
25-34 (N=239)	57.3	60.7	10.0	31.0	8.8	2.5	4.6	38.5
35-44 (N=184)	58.2	57.6	17.4	23.9	6.5	7.1	2.2	27.7
45-54 (N=126)	42.9	44.4	20.6	23.8	7.9	4.8	4.0	23.0
55 and Over (N=64)	35.9	31.3	18.8	15.6	7.8	0.0	3.1	18.8

* = p < .05, ** = p < .01, *** = p < .001

The information in Table 12 shows the various tactics used most often by demographic groups in the cases reviewed. The information suggests that older offenders prefer cyber tactics that have been around for a longer period of time, including phone calls and e-mails, while

younger offenders prefer newer cyber tactics such as social networking. This suggests that offenders of stalking utilize the tools in which they are the most comfortable and/or have the most experience with.

Table 13 shows the distributions of offender and victim demographics with case outcomes. According to the results, offender gender and victim gender were significant with arrest. Male offenders had arrest rates of 30.5%, while female offenders had arrest rates of 13.6%. Additionally, cases with male victims had arrest rates of 15.8% and those with female victims had arrest rates of 25.2%. Table 1 had shown that the majority of cases involved male offenders and female victims independently, but Table 13 shows that when the offenders are female and the victims are male, the arrest rates were lower and the results were significant.

While not significant, the table also provides other notable patterns. Table 13 shows that of the cases reported, those in which the offender was white had arrest rates of 27.1% and those in which the offender was black had arrest rates of 27.7%. Of the cases that went to trial, those with white offenders had trial rates of 39.0% and those with black offenders had trial rates of 40.4%, and the guilty verdicts were 91.1% for white offenders and 95.8% for black offenders. Overall, black offenders had higher rates of arrest, trial, and guilty verdicts than white offenders.

For the cases that continued to trial, male offenders had trial rates of 38.9% and guilty verdict rates of 93.2%, compared to female offenders that had trial rates of 35.0% and guilty verdict rates of 85.7%. The table shows that female offenders had lower trial rates and guilty verdicts than male offenders.

Offenders who were under 18 at the time of the report had arrest rates of 25.0% and trial rates of 0.0%, resulting in no opportunity for guilty verdicts. Offenders between the ages of 18 and 24 had arrest rates of 25.0%, trial rates of 26.9%, and 85.7% guilty verdicts. For the

offenders who were between the ages of 25 and 34, the arrest rates were 29.7%, the trial rates were 36.6%, and 88.0% had guilty verdicts. Offenders between the ages of 35 and 44 had arrest rates of 31.0%, trial rates of 46.6%, and 92.6% resulted in guilty verdicts. Of the offenders who were between the ages of 45 and 54, the arrest rates were 28.6%, the trial rates were 38.9%, and 100.0% had guilty verdicts. Offenders over the age of 55 had arrest rates of 23.4%, trial rates of 33.3%, and 100.0% had guilty verdicts. Overall, offenders between the ages of 34 and 44 had the highest arrest rates as well as the highest trial rates. However, offenders between the ages of 45 and 54 and 55 and over had the highest rates of guilty verdicts.

Additionally, the results in Table 13 show that cases with white victims had arrest rates of 24.3% and cases with black victims had arrest rates of 18.9%. The results also show that of the cases that resulted in arrest, those with white victims had 37.9% trial rates and those with black victims had 44.4% trial rates. Additionally, of the cases that went to a judge or jury, the cases with white victims resulted in guilty verdicts 93.1% of the time and the cases with black victims resulted in guilty verdicts 91.7% of the time. According to the table, cases with white victims had the highest arrest and guilty verdict rates, while cases with black victims had the highest trial rates.

Of those that went to trial, the cases with male victims had 47.8% trial rates and 100.0% guilty verdicts and the cases with female victims had 38.3% trial rates and 91.8% guilty verdicts. Interestingly, cases with male victims had higher trial rates and guilty verdicts than cases with female victims.

In cases where the victims were under the age of 18, the arrest rates were 31.3%, the trial rates were 40.0%, and 100.0% resulted in guilty verdicts. When the victims were between the ages of 18 and 24, the arrest rates were 23.1%, the trial rates were 21.4%, and 83.3% had guilty

verdicts. For the cases with victims between the ages of 25 and 34, the arrest rates were 22.0%, the trial rates were 43.2%, and 93.8% received guilty verdicts. In the cases in which the victims were between the ages of 35 and 44, the arrest rates were 24.8%, the trial rates were 53.1%, and 100.0% resulted in guilty verdicts. The cases with victims between the ages of 45 and 54 had arrest rates of 28.2%, trial rates of 41.7%, and 100.0% had guilty verdicts. Additionally, when the victims were over the age of 55, the arrest rates were 23.8%, the trial rates were 20.0%, and 100.0% resulted in guilty verdicts. Overall, the cases with victims under the age of 18 had the highest arrest rates, while cases with victims between the ages of 35 and 44 had the highest trial rates. The rates of guilty verdicts were even at 100.0% for offenders under the age of 18, and between the ages of 35 and 44, 45 and 54, and 55 and over.

Table 13 Outcomes of Reported Stalking Offenses by Demographics

	Arrest % (N=884)	Trial % (N=213)	Guilty % (N=80)
Offender Race			
White	27.1	39.0	91.1
Black	27.7	40.4	95.8
Offender Gender			
Male	30.5***	38.9	93.2
Female	13.6***	35.0	85.7
Offender Age			
Under 18	25.0	0.0	N/A
18-24	25.0	26.9	85.7
25-34	29.7	36.6	88.0
35-44	31.0	46.6	92.6
45-54	28.6	38.9	100.0
55 and Over	23.4	33.3	100.0
Victim Race			
White	24.3	37.9	93.1
Black	18.9	44.4	91.7
Victim Gender			
Male	15.8**	47.8	100.0
Female	25.2**	38.3	91.8
Victim Age			
Under 18	31.3	40.0	100.0
18-24	23.1	21.4	83.3
25-34	22.0	43.2	93.8
35-44	24.8	53.1	100.0
45-54	28.2	41.7	100.0
55 and Over	23.8	20.0	100.0

* = $p < .05$, ** = $p < .01$, *** = $p < .001$

Table 14 presents the chi-square statistics between mode, relationship, direct threats, and victim action, as well as tactics phone call, text message, e-mail, social networking, video/photo,

tracking device, doxing, and total methods with arrest, trial, and guilty verdict. As the various tactic and total methods variables were only utilized in cyber cases and combination cases, they were each examined by selecting only the cyber cases and combination cases to ensure the in-person cases did not impact the results.

Based on the chi-square statistics presented in Table 14, I reject the null hypotheses that no relationship exists between arrest and mode, relationship, direct threats, victim action, phone call, social networking, doxing, and total methods independently. In addition, based on the chi-square statistics, I also reject the null hypotheses that no relationship exists between trial and mode and relationship independently, as well as trial and phone calls in combination cases. I further reject the null hypothesis that no relationship exists between guilty verdict and phone call and social networking independently based on the chi-square statistic, as well as guilty verdicts and phone calls and social networking independently.

Table 14 Bivariate Results for Chi-Square Test of Various Independent Variables and Arrest, Trial, and Guilty Verdict

	Arrest	Trial	Guilty Verdict
Mode	.000***	.018*	.191
Relationship	.000***	.047*	.717
Direct Threats	.004**	.598	.651
Victim Action	.000***	.517	.929
Phone Call	.013*	.076	.125
Cyber Cases	.025*	.253	N/A
Combination Cases	.050*	.050*	.010**

Table 14 Bivariate Results for Chi-Square Test of Various Independent Variables and Arrest, Trial, and Guilty Verdict

	Arrest	Trial	Guilty Verdict
Text Message	.673	.793	.899
Cyber Cases	.653	.517	N/A
Combination Cases	.762	.419	.593
E-Mail	.402	.200	.285
Cyber Cases	.190	.111	N/A
Combination Cases	.142	.590	.515
Social Networking	.001***	.759	.093
Cyber Cases	.082	.253	N/A
Combination Cases	.141	.508	.029*
Video/Photo	.682	.424	.396
Cyber Cases	.825	.976	N/A
Combination Cases	.247	.722	.515
Tracking Device	.304	.318	.774
Cyber Cases	.271	N/A	N/A
Combination Cases	.204	.518	.716
Doxing	.047*	.619	.683
Cyber Cases	.202	.882	N/A
Combination Cases	.735	.578	.716
Total Methods	.044*	.717	.978
Cyber Cases	.065	.483	N/A
Combination Cases	.095	.614	.882

* = $p < .05$, ** = $p < .01$, *** = $p < .001$

The results of the bivariate analyses shown in Table 14 indicate that the social networking, doxing, and total methods variables were significant when all cases were considered, but not when face-to-face cases were removed and cyber and combination cases were separated. Additionally, the mode, relationship, direct threat, and victim action variables were all significantly correlated with arrest, but only mode and relationship were correlated with

trial and none of the four variables were correlated with guilty verdicts. The results show that a number of factors appear to impact law enforcement officers' decision to arrest, but not prosecutors' decision to take cases to or completely through trial.

Multivariate Analysis

Table 15 provides the results of the logistic regression conducted between the mode used by offenders and whether an arrest was made or charges were filed. Multivariate analyses with trial and guilty verdicts were not conducted as there were not enough cases that proceeded to trial to evaluate. The model predicts the odds of an arrest by the mode used. The Cox & Snell R Square statistic is .031 and indicates that the model is only slightly better than the intercept only model. The chi-square statistic for this logistic regression is 27.887 and is significant at the $p < .001$ level. The tolerances are within acceptable levels and do not raise concerns about multicollinearity, showing that the model as a complete group of variables provides a significantly better understanding of the dependent variable's variation than a random model. According to the results, the odds of arrest are 132.4% greater for face-to-face stalking than cyber stalking. Additionally, the results show that the odds of arrest are 155.5% higher for offender who utilize both cyber and face-to-face tactics than those who use cyber tactics alone.

Table 15 Logistic Regression Results of Mode and Arrest

	b	S.E.	Exp (B)	Tolerance
Mode				
Cyber	Constant	-	-	-
Face-to-Face	.843	-.228	2.324***	.848
Combination	.938	-.191	2.555***	.848

* = p < .05, ** = p < .01, *** = p < .001
Cox & Snell: .031 -2 log likelihood: 946.053 Chi-square: 27.887***

Table 16 highlights the logistic regression models for the arrest of offenders and various independent variables that had significant chi-square values in the bivariate models. The models for these logistic regressions are split by the mode used by offenders. Model 1 includes cyber only cases, Model 2 includes face-to-face on cases, Model 3 includes combination cases, and Model 4 includes all cases. Before the logistic regressions were completed, a check for multicollinearity was conducted and determined that the correlation between the offender's gender and the victim's gender was significant and therefore the victim's gender variable was removed from the models. The models predict the odds of an offender of stalking being arrested with the following independent variables: direct threats, victim proactive, and offender gender. The Cox & Snell R Square statistics for the models, (.031, .046, .126, and .054) indicate that the models are only slightly more improved than the intercept only models. The chi-square value for Model 1 was 8.503 and was significant at the $p < .05$ level and the chi-square value for Model 2 was 6.835, but was not significant. Due to the chi-square value for Model 2 not being significant, the results from Model 2 were not interpreted. The chi-square value for Model 3 was 47.003 and for Model 4 was 42.552 and both were significant at the $p < .001$ level. The tolerances are within acceptable levels and do not raise concerns about multicollinearity.

The logistic regressions show that the odds of cases having an arrest or charges being filed were 189.6% greater for those that included direct threats in combination cases, or those that involved both cyber and face-to-face stalking methods. The results also show that the odds of arrest or charges being filed were 68.9% higher for those that included direct threats in stalking cases of all methods. The logistic regressions indicate that the odds of arrest or charges being filed were 137.9%, 150.5%, and 83.0% greater for those in which the victims took proactive measures in cyber cases, combination cases, and all cases respectively. In addition, the models show that the odds of arrest or charges being filed were 87.5% and 62.9% less for those that involved female offenders in combination cases and all cases.

Table 16 Logistic Regression Results of Various Independent Variables and Arrest by Mode

	b	S.E.	Exp (B)	Tolerance
Direct Threats				
Cyber Cases	.212	(.337)	1.236	.990
Face-to-Face Cases	.123	(.520)	1.131	.995
Combination Cases	1.063	(.251)	2.896***	.995
All Cases	.524	(.174)	1.689**	.998
Victim Action				
Cyber Cases	.867	(.355)	2.379*	.990
Face-to-Face Cases	.918	(.360)	2.505*	.998
Combination Cases	.604	(.264)	1.830*	.979
All Cases	.677	(.174)	1.968***	.995
Offender Gender				
Cyber Cases	-.590	(.443)	.554	1.000
Face-to-Face Cases	-.203	(.455)	.817	.997
Combination Cases	-2.088	(.542)	.124***	.983
All Cases	-.991	(.259)	.371***	.996

* = p < .05, ** = p < .01, *** = p < .001

Cyber Cases:	Cox & Snell: .031	-2 log likelihood: 244.612	Chi-square: 8.503*
Face-to-face Cases:	Cox & Snell: .046	-2 log likelihood: 179.486	Chi-square: 6.835
Combination Cases:	Cox & Snell: .126	-2 log likelihood: 391.806	Chi-square: 47.003***
All Cases:	Cox & Snell: .054	-2 log likelihood: 855.943	Chi-square: 42.552***

Table 17 includes the logistic regression models for arrest and the relationship between the offenders and victims. As in the previous models, the models were split by the mode, with Model 1 including cyber cases, Model 2 including face-to-face cases, Model 3 including combination cases, and Model 4 including all cases. In order to compare the odds of arrest for the various relationships, dummy variables were created for each relationship. The logistic regressions were conducted with the partner relationship acting as the constant due to partner having the highest frequency value in each model. The Cox & Snell R Square statistics for the models (.091, .101, .087, and .083) indicate that the models are only slightly more improved than the intercept only models. The chi-square values for the models were 30.771, 17.832, 33.282, and 73.931 respectively, with all models being significant at the $p < .001$ level with the exception of Model 2 which was significant at the $p < .05$ level. The tolerances are within acceptable levels and do not raise concerns about multicollinearity.

Table 17 Logistic Regression Results of Relationship and Arrest by Mode

	b	S.E.	Exp (B)	Tolerance
Relationship				
Spouse				
Cyber Cases	.123	.491	1.131	.891
Face-to-Face Cases	.609	.619	1.838	.772
Combination Cases	.175	.321	1.191	.907
All Cases	.258	.243	1.294	.878
Family Member				
Cyber Cases	-.383	.810	.682	.947
Face-to-Face Cases	N/A	N/A	N/A	N/A
Combination Cases	.596	1.102	1.815	.989
All Cases	-.382	.584	.683	.971

Table 17 Logistic Regression Results of Relationship and Arrest by Mode

	b	S.E.	Exp (B)	Tolerance
Co-Worker				
Cyber Cases	-1.181	1.07	.307	.947
Face-to-Face Cases	-.526	.869	.591	.837
Combination Cases	-.097	.569	.908	.964
All Cases	-.456	.418	.634	.943
Neighbor				
Cyber Cases	N/A	N/A	N/A	N/A
Face-to-Face Cases	-.190	.568	.827	.690
Combination Cases	-.097	1.234	.908	.992
All Cases	-.382	.421	.683	.946
Ex of Partner/Partner of Ex				
Cyber Cases	-1.712	1.051	.181	.919
Face-to-Face Cases	N/A	N/A	N/A	N/A
Combination Cases	N/A	N/A	N/A	N/A
All Cases	-2.892	1.019	.055**	.937
Acquaintance				
Cyber Cases	-.860	.434	.423*	.806
Face-to-Face Cases	.167	.616	1.182	.754
Combination Cases	-.695	.374	.499	.909
All Cases	-.685	.251	.504**	.849
Stranger				
Cyber Cases	-2.211	1.04	.110*	.882
Face-to-Face Cases	.247	.498	1.280	.642
Combination Cases	-.908	.574	.403	.950
All Cases	-.561	.289	.571	.884
Partner				
Cyber Cases	Constant	-	-	-
Face-to-Face Cases	Constant	-	-	-
Combination Cases	Constant	-	-	-
All Cases	Constant	-	-	-

* = p < .05, ** = p < .01, *** = p < .001

Cyber Cases:	Cox & Snell: .091	-2 log likelihood: 244.200	Chi-square: 30.771***
Face-to-face Cases:	Cox & Snell: .101	-2 log likelihood: 178.762	Chi-square: 17.832*
Combination Cases:	Cox & Snell: .087	-2 log likelihood: 411.798	Chi-square: 33.282***
All Cases:	Cox & Snell: .083	-2 log likelihood: 865.640	Chi-square: 73.931***

The results in Table 17 show that the victim and offender relationships were not significant predictors of arrest, except for cyber cases that involved strangers or acquaintances. In cases in which offenders used only cyber tactics, both strangers and acquaintances had lower odds of being arrested. These results show that law enforcement officers may not view cyber stalking cases in which the victim and offender do not know each other well, or even at all, as being able to cause the level of emotional distress necessary to constitute stalking.

The multivariate analyses show that the odds of arrest were greatest for combination cases, followed by face-to-face cases, with cyber cases having the lowest odds of arrest. The analyses also show that direct threats and male offenders resulted in greater odds of arrest for combination cases. Additionally, victim action in cases resulted in higher odds of arrest in cases regardless of the mode of stalking. The multivariate analyses also show that the relationship between the offender and victim was only significant for acquaintances and strangers in cyber cases, and resulted in lower odds of arrest when compared to partners.

CHAPTER 6: DISCUSSION

The purpose of this study was to determine the various factors that impact law enforcement and prosecutorial actions in cyber stalking cases through the lens of rational choice theory. This study aimed to assess the theory's ability to increase our understanding of how decisions about cyber stalking cases are made by the actors within the criminal justice system. In doing so, the current study examines a variety of independent variables, including mode of stalking and tactics used by offenders, actions taken by victims, and demographic characteristics of offenders and victims and how they relate to dependent outcome variables, including arrest of the offenders or charges filed by the prosecutors, whether the cases went to trial, and verdicts.

The results of this study show that the majority of offenders in the cases examined were white, male, and between the ages of 25 and 34. Additionally, the majority of victims in these cases were white, female, and also between the ages of 25 and 34. These results were the same across the modes of stalking, including cyber only, face-to-face only, and a combination of both. The study also shows that the majority of cases involved both cyber and stalking components, with cyber only cases being the next highest and face-to-face only being the lowest.

The study also found that the majority of cases did not involve direct threats against the victims, phone calls, e-mails, social networking, video/photos, tracking devices, or doxing. Most of the victims and offenders in these cases were at some point considered partners, whether current or ex. Also, victims took action to stop the offender in the majority of cyber and combination cases, but did not take action in the majority of face-to-face cases.

Overall, only 24.0% of cases resulted in arrests or charges against offenders. Of those who had arrests or charges, only 38.0% of cases went to trial. However, of the cases that went to

trial, 92.5% resulted in a guilty verdict, with 100.0% of cyber cases that went to trial ending in a guilty verdict.

The study shows that the odds of arrest or charges are greatest for offenders who utilize both cyber and face-to-face tactics followed by those who use face-to-face methods alone. Offenders who stalked their victims through cyber tactics alone had the lowest odds of arrest. These results show that law enforcement officers and prosecutors may feel as though offenders who stalk their victims both face-to-face and electronically pose the greatest threat to victims. Alternatively, this may also mean that the combination of face-to-face and cyber methods show that the behaviors cause "substantial emotional distress" as required in the legal definition of stalking in Florida (FLA STAT. ANN. § 784.048(d)). On the opposite end of the spectrum, the results show that law enforcement officers and prosecutors may feel as though offenders who use only cyber means to stalk their victims may not pose a threat to their victims or cause emotional distress.

The current study examined the impact of direct threats, victim actions, and offender gender on the odds of arrest. The findings show that in all cases of stalking, cases involving direct threats, proactive victims, and male offenders have higher odds of arrests. Additionally, the results show that when the cases are split by mode, only victim action was a significant factor in the odds of arrest for cyber cases and face-to-face cases. However, all three variables, direct threats, victim proactive, and offender gender, were significant in combination cases.

These results show that for cyber cases, it appears that the only factor that impacted the odds of arrest was whether the victim took action. This may mean that law enforcement officers and prosecutors do not take the offender's gender or direct threats into account when making the decision to arrest or file charges. As these cases took place solely through electronic means, law

enforcement officers and prosecutors may believe that direct threats are unsubstantiated because the offenders have made no attempts to interact with the victims face-to-face. It is also possible that law enforcement officers and prosecutors do not believe that direct threats made electronically could cause the level of emotional distress necessary to meet definition of stalking. Law enforcement officers and prosecutors may not take into account the offender's gender in cyber stalking cases because they feel as though one gender does not pose a greater threat than another went the stalking is taking place virtually.

The victim action variable was significant in all of the cases regardless of the mode of stalking used. This may show that the emotional distress is more apparent when victims have taken action to stop the behaviors from continuing. Law enforcement officers and prosecutors may feel as though the cases are stronger if victims took measures to protect themselves and the offenders continued the behavior regardless. Additionally, law enforcement and prosecutors may feel as though victims will be more willing to participate in the criminal justice process if they have previously taken measures to protect themselves. This may mean that it could be important for advocates or other individuals who assist victims to help empower victims to act proactively to prevent future occurrences of stalking. Additionally, it could be important for victims to be aware of the importance of their proactive actions prior to reaching out to law enforcement to report the behavior. In addition, it may be helpful for law enforcement officers to encourage victims who have not taken proactive action to do so and to file an additional report if the behavior continues.

The results of the study also show that the relationships between the offenders and victims were only significant in cyber cases when it came to acquaintances and strangers. According to the findings, in cases where the offenders were acquaintances and strangers to the

victims, there was a lower probability of an arrest or having charges filed than in cases where offenders were partners. These results may show that law enforcement officers and prosecutors do not view acquaintances or strangers as being as threatening towards victims or causing significant levels of emotional distress due to their more distant relationships than those between partners. These findings may indicate that in cyber cases, victims may have no need to continue communication with acquaintances or strangers in the same way they may need to with partners, and therefore law enforcement officers and prosecutors may feel it would be easier for victims to distance themselves from stalkers they do not have continued relationships with.

When looking at the frequencies for the guilty verdicts, it is interesting to see that overall 92.5% of cases that went to trial resulted in guilty verdicts. This high number, along with the 100.0% result for cyber cases that had guilty verdicts, gives the impression that prosecutors only chose to move forward with cases they were extremely confident they would win. Of the 336 cyber cases that were reviewed, only 49 (14.6%) resulted in arrest and of those, 27 (55.1%) move forward to trial. While the majority of cyber cases that resulted in arrest made it all the way to trial, and subsequently had guilty verdicts, cyber cases had the lowest percentage of arrests or charges being filed initially, with face-to-face cases resulting in arrest 28.7% of the time and combination cases resulting in arrest 30.2% of the time. This shows that it may not be only the prosecutors who choose to only move forward with cyber cases they are confident they will win, but law enforcement officers also may not make arrests in cyber cases unless there is sufficient evidence to prove the case. Another interesting factor is that the majority of cases that proceeded to trial resulted in a bench trial with a judge instead of a jury trial. While not tracked in this study, it is possible that many of these cases had the same judges. This raises the question as to whether prosecutors take the judge into account when deciding whether or not to pursue stalking

cases. These results show rational choice theory in action. Both law enforcement officers and prosecutors appear to make rational decisions to move forward in adjudicating stalking cases based on their beliefs about how successful the cases will be in the judicial system.

The results of this study show some of the factors that influenced arrest and prosecutorial decisions. In particular, several of the variables measured showed significant relationships with the outcome of arrest or charges being filed. The majority of the variables measured did not appear to directly impact decisions by prosecutors to move cases forward to trial or whether the offenders would be found guilty at trial. The variables mode, direct threat, victim action, tracking device, and doxing correlated with the arrest outcome. However, when cases were split by mode, only the victim action variable impacted arrest outcomes in cases of cyber stalking. The results showed that very few cases of cyber stalking resulted in arrest and just over half of those arrested went to trial. However, all of the cyber cases that went to trial resulted in guilty verdicts, indicating the prosecutors only fully pursued cases of cyber stalking they knew they could win in court.

Limitations

This study is limited by the sample size and the availability of police reports to the researcher. The study is also limited to the geographical area of Central Florida, and would benefit by expanding to other jurisdictions for more variety. In addition, the study is limited to the information documented in the police reports and the Clerk of Court websites and does not include information directly from law enforcement officers or prosecutors regarding their decisions. Also, the information in the reports regarding race and ethnicity was inconsistent and

did not appear to be accurate. For example, one county did not include ethnicity in their reports and another county included Hispanic as a race instead of ethnicity. In the future, conversations with law enforcements officers and prosecutors regarding their decisions may be beneficial in order to gain a better understanding of the rational choices made in the criminal justice process. In addition, this study is also limited to modes of stalking that use technology versus those that do not. Although technology has advanced, some of the more traditional forms of stalking may have included technology, such as phone calls to landlines. However, due to the current nature of technology and the information available in the police reports, all forms of technology were considered "cyber," despite some potentially using more traditional methods. Despite these limitations, the study provides useful information regarding the factors that impact law enforcement and prosecutorial actions.

Conclusions

Previous research on cyber stalking primarily focused on the behaviors and decisions of offenders and victims, but not law enforcement and prosecutors. This study contributes to the previous research by adding some of the factors that influenced the rational choices and outcome decisions of actors within the criminal justice system. In particular, this study shows the importance of victims' actions in attempting to prevent occurrences of cyber stalking and the impact those actions have on arrest and prosecutorial decisions. These findings offer insight to law enforcement officers on how they may assist victims who report stalking. Law enforcement officers often have the opportunity to assist victims with taking proactive measures, such as filing for injunctions, blocking offenders, or informing offenders that they want contact to stop.

In the event that victims have not previously taken measures to stop the stalking behaviors, law enforcement officers may be able to encourage victims to re-report in the event that the behaviors continue. The results of this study show the importance of victim action in stalking cases, and law enforcement officers have the unique opportunity to encourage victim action to successfully adjudicate cases if offenders continue the behavior.

In the future, research should continue to examine the various factors that impact arrest and prosecutorial decisions. Also, future research will assist law enforcement officers to know what factors prosecutors are looking for when taking cases to trial, and to assist both law enforcement officers and prosecutors in having a better understanding of the various tactics used by offenders of stalking.

This study, while limited in scope, provides a snapshot into the outcomes of stalking cases as they relate to the tactics and methods used. As a researcher, I experienced frustration while reading the narratives of many of the reports and subsequently following up to see the outcomes. In a number of cases, the narratives did not describe cases that appeared to meet the basic definitions of stalking, in particular the requirement about significant emotional distress. For example, I recall a situation in which a neighbor placed dog excrement in his neighbor's driveway a total of three times. In this case, the neighbor was not only arrested for stalking, but was prosecuted and found guilty of the crime. Conversely, I also experienced frustration in reading some cases that seemed extremely volatile, but no arrest was made or charges were filed. I remember numerous cases that included threats to kill, some including photographs of firearms. In many of these cases, I recall feeling surprised in not finding that charges appeared on the Clerk of Courts website, but not shocked to see that the same offender and victim appeared in cases at a later date for behaviors that had escalated, including battery and breaking and entering.

In seeing the same offenders and victims appear multiple times in reports and again on the Clerk of Courts website for escalated crimes, it became clear that the reports to law enforcement did not prevent future occurrences or provide the protections the victims most likely believed they would receive. While reading these reports and reviewing the outcomes, it became apparent to me even before I knew the results, that decisions were being made not solely based on factors related to safety, but more so on the assumption from law enforcement officers and prosecutors that they had a solid case against the offenders. It is my hope that in the future, arrest and prosecutorial decisions are made not based on the win or lose game that is the criminal justice system, but for the protection of the victims who are being tormented by these offenders.

LIST OF REFERENCES

Al-Khateeb, H. M., Epiphaniou, G., Alhaboby, Z. A., Barnes, J., & Short, E. (2017). Cyberstalking: Investigating formal intervention and the role of Corporate Social Responsibility. *Telematics and Informatics*, *34*(4), 339-349.

Bandura, A., & Walters, R. H. (1977). *Social learning theory* (Vol. 1). Englewood Cliffs, NJ. Prentice Hall.

Beccaria, C. (2009). *On Crimes and Punishments.* Piscataway, NJ. Transaction Publishers (Original work published in 1764).

Bentham, J. (1996). *The collected works of Jeremy Bentham: An introduction to the principles of morals and legislation*. Oxford, UK. Clarendon Press (Original work published in 1789).

Bocij, P. (2003). Victims of cyberstalking: An exploratory study of harassment perpetrated via the Internet. *First Monday* 8(10).

Brewster, M. P. (2001). Legal Help-Seeking Experiences of Former Intimate-Stalking Victims. *Criminal Justice Policy Review*, *12*(2), 91-112.

Brown, C. S. (2015). Investigating and prosecuting cyber crime: Forensic dependencies and barriers to justice. *International Journal of Cyber Criminology*, *9*(1), 55.

Catalano, S. (2012). Stalking victims in the United States-revised. *Age*, *18*(19), 8-047.

Cavezza, C., & McEwan, T. E. (2014). Cyberstalking versus off-line stalking in a forensic sample. *Psychology, Crime & Law*, *20*(10), 955-970.

Chik, W. (2008). Harassment through the digital medium-a cross jurisdictional comparative analysis of the law on cyberstalking. *J. Int'l Com. L. & Tech.*, *3*, 13.

Clarke, R. V., & Cornish, D. B. (1985). Modeling offenders' decisions: A framework for research and policy. *Crime and justice* 6, 147-185.

Cohen, L. E., & Felson, M. (1979). Social change and crime rate trends: A routine activity approach. *American sociological review*, 588-608.

Cornish, D. B., & Clarke, R. V. (1987). Understanding crime displacement: An application of rational choice theory. *Criminology* 25(4), 933-948.

Davis, J. T. (2012). Examining perceptions of local law enforcement in the fight against crimes with a cyber component. *Policing: An International Journal of Police Strategies & Management 35*(2), 272-284.

DeMatteo, D., Wagage, S., & Fairfax-Columbo, J. (2017). Cyberstalking: are we on the same (web) page? A comparison of statutes, case law, and public perception. Journal of Aggression, *Conflict and Peace Research*, 9(2), 83-94.

Dreßing, H., Bailer, J., Anders, A., Wagner, H., & Gallas, C. (2014). Cyberstalking in a large sample of social network users: Prevalence, characteristics, and impact upon victims. *Cyberpsychology, Behavior, and Social Networking*, *17*(2), 61-67.

Diamond, B., & Bachmann, M. (2015). Out of the Beta Phase: Obstacles, Challenges, and Promising Paths in the Study of Cyber Criminology. *International Journal of Cyber Criminology 9*(1), 24.

Dogaru, O. (2012). Criminological Characteristics of Computer Crime. *Journal Of Criminal Investigation* 5(1), 92-98.

D'Ovidio, R., & Doyle, J. (2003). A study on cyberstalking: Understanding investigative hurdles. *FBI L. Enforcement Bull.*, *72*, 10.

Ferguson-Gilbert, C. (2001). It is not whether you win or lose, it is how you play the game: Is the win-loss scorekeeping mentality doing justice for prosecutors. *Cal. WL Rev.*, *38*, 283.

Finch, E. (2001). *The criminalisation of stalking: Constructing the problem and evaluating the solution*. Routledge-Cavendish.

Fisher, B. S., Cullen, F. T., & Turner, M. G. (2002). Being pursued: Stalking victimization in a national study of college women. *Criminology & Public Policy* 1(2), 257-308.

Fox, V. (1962). Toward an Understanding of Criminal Behavior. *The American Journal of Economics and Sociology*, (2). 145.

Furnell, S. (2002). *Cybercrime: Vandalizing the information society*. London: Addison-Wesley.

Geach, N., & Haralambous, N. (2009). Regulating harassment: is the law fit for the social networking age?. *The Journal of Criminal Law*, *73*(3), 241-257.

Gottfredson, M. R., & Hirschi, T. (1990). *A general theory of crime*. Stanford University Press.

Grabosky, P. N. (2001). Virtual criminality: old wine in new bottles?. *Social & Legal Studies 10*(2), 243-249.

Halder, D. & Jaishankar, K. (2012). *Cyber crime and the victimization of women: laws, rights and regulations*. Hershey, PA: Information Science Reference.

Holt, T. J., & Bossler, A. M. (2008). Examining the Applicability of Lifestyle-Routine Activities Theory for Cybercrime Victimization. *Deviant Behavior*, *30*(1), 1-25.

Jordan, C. E., Logan, T. K., Walker, R., & Nigoff, A. (2003). Stalking: An examination of the criminal justice response. *Journal of Interpersonal Violence*, *18*(2), 148-165.

Kane, R. J. (2000). Police responses to restraining orders in domestic violence incidents: Identifying the custody-threshold thesis. *Criminal Justice and Behavior*, *27*(5), 561-580.

Katyal, N. K. (2001). Criminal law in cyberspace. *University of Pennsylvania Law Review*, *149*(4), 1003-1114.

Kraft, E., & Wang, J. (2010). An exploratory study of the cyberbullying and cyberstalking experiences and factors related to victimization of students at a public liberal arts college. *International Journal of Technoethics* (IJT), 1(4), 74-91.

Landhus, J., (2018). Technology Facilitated Stalking. *Training and Technical Assistance Institute.* June 13-15, 2018. Fort Worth, Texas.

Levack, B. P. (1996). Possession, Witchcraft, and the Law in Jacobean England. *Washington and Lee Law Review*, *52*(5), 1613.

Logan, T., & Cole, J. (2007). The Impact of Partner Stalking on Mental Health and Protective Order Outcomes over Time. *Violence and Victims*, *22*(5), 546.

Logan, T. K., Nigoff, A., Walker, R., & Jordon, C. (2002). Stalker profiles with and without protective orders: reoffending or criminal justice processing?. *Violence and Victims*, *17*(5), 541.

Logan, T. K., & Walker, R. (2017). Stalking: A multidimensional framework for assessment and safety planning. *Trauma, Violence, & Abuse*, *18*(2), 200-222.

Lucks, B. D. (2004). Cyberstalking: Identifying and examining electronic crime in cyberspace (Doctoral dissertation, Alliant International University, California School of Professional Psychology, San Diego).

Lupsha, P. (1996). Transnational organized crime versus the nation-state. *Transnational Organized Crime 2*(1), 21-48.

Maple, C., Short, E., & Brown, A. (2011). Cyberstalking in the United Kingdom: An analysis of the ECHO pilot survey. University of Bedfordshire.

Marcum, C. D., & Higgins, G. E. (2019). Examining the Effectiveness of Academic Scholarship on the Fight Against Cyberbullying and Cyberstalking. *American Journal of Criminal Justice*, 1-11.

Meloy, J. R. (1998). The psychology of stalking. The psychology of stalking: *Clinical and forensic perspectives* 1-23.

Ménard, K. S., & Pincus, A. L. (2012). Predicting overt and cyber stalking perpetration by male and female college students. *Journal of Interpersonal Violence* 27(11), 2183-2207.

Ngo, F. T., & Paternoster, R. (2016). Toward an understanding of the emotional and behavioral reactions to stalking: A partial test of general strain theory. *Crime & Delinquency*, *62*(6), 703-727.

Owens, J. G. (2016). Why definitions matter: Stalking victimization in the United States. *Journal of interpersonal violence,* 31(12), 2196-2226.

Reyns, B. W., Henson, B., & Fisher, B. S. (2012). Stalking in the twilight zone: Extent of cyberstalking victimization and offending among college students. *Deviant Behavior*, 33(1), 1-25.

Shavers, B. (2013). *Placing the suspect behind the keyboard: using digital forensics and investigative techniques to identify cybercrime suspects.* Newnes.

Sheridan, L. P., & Grant, T. (2007). Is cyberstalking different? *Psychology, crime & law* 13(6), 627-640.

Shimizu, A. (2013). Domestic violence in the digital age: Towards the creation of a comprehensive cyberstalking statute. *Berkeley J. Gender L. & Just.*, *28*, 116.

Spitzberg, B. H. (2002). The tactical topography of stalking victimization and management. *Trauma, Violence, & Abuse*, *3*(4), 261-288.

Spitzberg, B. H., & Hoobler, G. (2002). Cyberstalking and the technologies of interpersonal terrorism. *New Media & Society* 4(1), 71-92.

Stephen, G. (1995). Crime in cyberspace. *The Futurist* 29(5), 24.

Strawhun, J., Adams, N., & Huss, M. T. (2013). The assessment of cyberstalking: An expanded examination including social networking, attachment, jealousy, and anger in relation to violence and abuse. *Violence and Victims, 28*(4), 715-730.

Vasiu, I., & Vasiu, L. (2016). Light My Fire: A Roentgenogram of Cyberstalking Cases. *American Journal of Trial Advocacy*, 40, 41.

Wall, D. S. (1999). Cybercrimes: New wine, no bottles. *Invisible crimes: Their victims and their regulation*, 105-39.

Westera, N. J., & Powell, M. B. (2017). Prosecutors' perceptions of how to improve the quality of evidence in domestic violence cases. *Policing and society*, *27*(2), 157-172.

Willits, D., & Nowacki, J. (2016). The use of specialized cybercrime policing units: An organizational analysis. *Criminal justice studies*, *29*(2), 105-124.

Yar, M. (2005). The Novelty of 'Cybercrime' An Assessment in Light of Routine Activity Theory. *European Journal of Criminology 2*(4), 407-427.

Zhigang, Y. (2011). Cyber variants of traditional crimes and criminal law responses. *Social Sciences in China 32*(1), 66-79.