UNDERSTANDING AND PREDICTING CYBERSTALKING IN SOCIAL MEDIA: INTEGRATING THEORETICAL PERSPECTIVES ON SHAME, NEUTRALIZATION, SELF-CONTROL, RATIONAL CHOICE, AND SOCIAL LEARNING

Written by ***Dr. S. Krishnan Mani* & Dr. Niharika Gaur*****,

** Assistant Professor, Seedling School of Law and Governance, Jaipur National University*

*** Assistant Professor, Seedling School of Law and Governance, Jaipur National University*

ABSTRACT

Cyberstalking has received increasing attention in academia and the public for its pervasive effect on society. However, there has been little comprehensive research concerning the mechanisms of cyberstalking behavior, particularly in social media. In this article, we define cyberstalking and explain how it is dramatically different from real-world stalking, and thus calls for additional taxonomic and theoretical development. Based on an extensive review of the literature and case studies of cyberstalking, we then propose a comprehensive taxonomy of cyberstalking. On this basis, we develop a theoretical model to explain and predict cyberstalking behavior. To better understand cyberstalking, we propose a model that integrates five theories within three levels of prediction: the intrapersonal level (emotional theory, neutralization theory, and self-control theory), the situational level (rational choice theory), and the interpersonal level (social learning theory). On this taxonomic and theoretical foundation, future empirical research should be able to further explain, predict, and test cyberstalking behavior online.

KEYWORDS: Stalking, Cyberstalking, Shame, Neutralization, Self-control, Rational choice theory

INTRODUCTION

With the development of online communication information technology (IT), it is increasingly difficult to protect users from online stalking (D'Ovidio & Doyle, 2003). In the age of social media, cyberstalking behavior is increasingly ubiquitous and serious. The media has widely reported cyberstalking instances of identity theft, online impersonation, identity deception, threats, and hostile posting, that is, posting false information intended to cause harm (Maple et al., 2011), as well as the newer, insidious twists of the posting of "revenge porn" by jilted lovers (Melnicoe, 2013; Miller, 2013) and ill-intentioned groups of online teens bullying victims into suicide (Liston, 2013). Furthermore, cyberstalking is becoming increasingly more common than offline stalking (McVeigh, 2011). Maple et al. (2011) showed that cyberstalking is becoming progressively more prevalent in social media. Because of its widespread effect on the psychology, finances, and social interactions of individuals, cyberstalking not only hurts victims psychologically, but also influences their work and even their relationships with friends and family.

The prevalence, nature, and negative social consequences of cyberstalking have led to growing public concern regarding its presence in the online environment (as shown in Appendix A). Because social media encourages users to exchange information within the community, as well as to use new features and applications that expose additional personal information (Ellison, 2007), it provides a new, effective, and efficient means to perform stalking behavior at the expense of a relatively large number of potential victims. First, the large network size, combined with the numerous privacy leaks in public networks, make it

extremely convenient for individuals to unethically, unlawfully, or immorally stalk others using social media tools. Therefore, even people with very little IT competence have the potential to become cyberstalkers (Costa, 2012). Furthermore, because social media features a wide range of relationships, stalkers from the cyberworld vary from intimate friends to strangers (Gutierrez, 2013; Lyndon et al., 2011). With a strong need to use social media and self-disclose online, typical users often lack the ability or sufficient concern to manage and protect their privacy online, thus leading to a clash between the risks and benefits of online activities (Gross & Acquisti, 2005).

Given the huge, increasing negative impact cyberstalking and cyberbullying has on society, it has drawn highly interdisciplinary research interest. Information systems (IS) literature on cyberstalking has focused primarily on analyzing its ethical and moral aspects and the legal responsibility of the different participants (Tavani & Grodzinsky, 2002). Adam (2002) highlighted the role of gender in analyzing cyberethics problems and maintained that third-party cyberstalking should receive more attention. Grodzinsky and Tavani (2002) argued that both Internet service providers and individual online users should assume moral responsibility, although in different ways. IS research on cyberbullying has emphasized the demographic antecedents that potentially predict cyberbullying. Scholars have explored the role of gender difference and the use of IT in cyberbullying (Erdur-Baker, 2010; Huang & Chou, 2010). Similarly, Tokunaga (2010) discussed how age and gender influence cyberbullying behavior and its possible psychosocial, affective, and academic consequences. Vandebosch and Van Cleemput (2009) investigated the influence of socio-demographics, psychosocial factors, and the usage of information communication technology on different roles (victims, bystanders, and bullies) in cyberbullying.

In media and communication research, scholars have attempted to measure cyberstalking to develop effective strategies to blunt it. For instance, Spitzberg and Rhea (1999) developed the scale of cyber-obsessional pursuit, which included four components (hyperintimacy, sabotage, invasion, and threat) that can be used to measure cyberstalking behavior. Spitzberg and Cupach (2001) further refined the measure of cyberstalking victimization and explored the incidence of such victimization. Spitzberg and Hoobler (2002) indicated that cyberstalking is experienced by a nontrivial proportion of undergraduate communication students and that there are weak but generally consistent relationships between facets of cyberstalking and real-world stalking.

Cyberstalking is also addressed in the disciplines of psychology and psychiatry. Boon and Sheridan (2002), for example, found that cyberstalking problems influenced mainly children and young people and that stalking behaviors are less likely to be performed by people with psychotic illnesses than by those with nonpsychotic illnesses. Zur et al. (2009) provided advice regarding the self-disclosure of psychotherapists in response to clients' online behaviors, including cyberstalking. Finally, Ybarra (2004) found that students who reported depressive symptomatology were more likely to be victims of cyberbullying, and the findings of Patchin and Hinduja (2010) indicated that cyberbullying leads to low self-esteem for both victims and offenders.

In general, cyberstalking is of great interest in interdisciplinary research and has been studied from many perspectives. However, most of the extant research has limited its focus to specific categories of cyberstalking behaviors, general measurement, descriptive studies, and exploratory studies. A large portion of the literature has focused, for example, on exploring cyberbullying behaviors of juveniles, or on children as the victims of Internet predators, while

ignoring the richer, broader range of cyberstalking behaviors and the reality that adults actively engage in both cyberbullying and cyberstalking behaviors. Little research has thus considered the underlying causal mechanisms and technologies that promote or blunt cyberstalking, especially among adult social media users. Given the currently scattered approaches to taxonomy and nomenclature in cyberstalking, it is not surprising that theoretical development in this area is immature.

We aim to help improve theorizing in this area, which must depart from theorizing in real-world stalking. In contrast with traditional stalking behavior, not every aspect of cyberstalking is purely negative and most cyberstalking cases do not actually constitute crimes (Campbell, 2012; Langer, 2013; Main, 2010). Indeed, many cyberstalking behaviors are performed without an immediate intention to harm the victim. The cyberstalker may just want to know more about or build a relationship with the victim, at least in the beginning. Thus, criminological theories, such as general deterrence theory (D'Arcy & Herath, 2011; Nagin & Pogarsky, 2001), probably cannot fully explain the widespread phenomenon of cyberstalking.

Furthermore, because cyberstalking is performed in a relatively low-risk context (i.e., often anonymously and at great physical distance), the technological attributes of the crime make it difficult for stalkers to be punished (Bocij & McFarlane, 2003). As a result, morality and ethics might be more important factors in explaining cyberstalking because it operates with few social and legal constraints. In the few studies that have addressed cyberstalking, it has been explained primarily from the perspective of personality or reasoned action. None of the various facets of this issue has been investigated with coherent intrapersonal, interpersonal, or situational models, or with a strong focus on ethics. Hence, it is imperative to investigate

systematically the process and possible antecedents of cyberstalking occurring in social media, thereby providing insights to support the more effective prevention, on the part of both operators and users, of cyberstalking in social media.

To fill this research gap, this study develops an integrative contextual theory to explain cyberstalking. We first define cyberstalking in general and develop a taxonomy of cyberstalking. With this taxonomy as a foundation, we then propose a theoretical model to explain and predict cyberstalking behavior. This model integrates five theories within three levels: the intrapersonal level (emotional theory, neutralization theory, and self-control theory), the situational level (rational choice theory), and the interpersonal level (social learning theory). Specifically, we integrate the most relevant explanatory variables from the five theories into a coherent model with specific propositions that can be operationalized into hypotheses through empirical work.

BACKGROUND ON AND TAXONOMY OF CYBERSTALKING

A common nomenclature and taxonomy is crucial to the development of a useful theory because they provide a proper conceptual foundation (Lowry et al., 2004; Posey et al., 2013). Consequently, in this section, we develop the foundation for the term *cyberstalking* and discuss the term in the context of social media. Because cyberstalking is a relatively recent phenomenon, we initiate our discussion of cyberstalking by situating it in relation to key features of traditional stalking. On this basis, we propose the taxonomy of cyberstalking that will be used to develop our theoretical model.

CYBERSTALKING AND TRADITIONAL STALKING

The term *cyberstalking* derives from stalking literature and generally refers to stalking that occurs in a cyberworld context. To understand the nature of cyberstalking behavior, we thus provide a clear definition of traditional stalking. Scholars have attempted to define stalking behavior from different perspectives, such as psychology, psychiatry, law, and criminology (Fisher et al., 2002; Kamphuis & Emmelkamp, 2000; Meloy, 2001; Palarea et al., 1999). However, there is no consensus on the exact definition of cyberstalking (Fukuchi, 2011; Sheridan & Davies, 2001; Stocker & Nielssen, 2000). Because this study primarily addresses the underlying mechanism of cyberstalking behaviors, we exclude the legal perspective and focus on stalking research from psychology and criminology.

We offer a few major definitions of stalking from the literature. From a psychological perspective, Meloy and Gothard (1995, p. 258) defined *stalking* as "the willful, malicious and repeated following and harassing of another person that threatens his or her safety." Westrup and Fremouw (1998, p. 258) suggested a behavioral-oriented definition: "one or more of a constellation of behaviors that (a) are repeatedly directed toward a specific individual, (b) are unwelcome and intrusive, and (c) induce fear or concern in the target." In criminology, Fisher et al. (2002, p. 255) defined it as "the same person exhibiting repeated pursuit behavior that seemed obsessive and made the respondent afraid or concerned for her safety." In a survey supported by the American National Institute of Justice et al. (1998, p. 240), stalking was defined as "a course of conduct directed at a specific person that involves repeated visual or physical proximity, nonconsensual communication, or verbal, written or implied threats, or a combination thereof, that would cause a reasonable person fear."

Most of these definitions contain three elements, as noted by Meloy (2001): (1) a behavioral intrusion on another person; (2) implicit or explicit threats arising from the

behavioral intrusion; (3) fear arising as a result of the threats. However, what we believe is missing in this synopsis is the foundational element of stalking: "stalkers are motivated by an obsession with having power, control, and influence over their victim" (Pittaro, 2007, p. 180). In line with these points, we define *stalking* as a series of repeated socially intrusive behaviors—motivated by an obsession with having power, control, and influence over a victim—that facilitate implicit and explicit threats, and thus induce fear in a victim.

Traditionalists such as Adam (2002) have argued that there is no substantive distinction between cyberstalking and stalking. In contrast, *uniqueness advocates* such as Tavani (2002) have claimed that because the scale and scope of cyberstalking are larger than those of traditional stalking, cyberstalking can result in special problems that have not appeared in traditional stalking. Although simplistic definitions of cyberstalking characterize it as traditional stalking performed via online media, our careful review of the literature and case studies of cyberstalking leads us to agree strongly with the uniqueness advocates for several important reasons.

First, Internet technologies and social media currently enable cyberstalkers to gain access to vast quantities of personal information (Basu & Jones, 2007), which makes stalking harder to prevent and the consequences for victims more serious than before (Fisher et al., 2002). Although cyberstalking was previously possible with email, chat rooms, and short message service (SMS), social media has further facilitated cyberstalking because of its richness and high volume of personal content. Social media encourages its users to exchange socially rich information with high levels of interactivity; the easy access to private information may thus expose users to data leaks (Ellison, 2007). The social connectedness enabled by such media, combined with the leaks of private data, makes it more difficult for users to protect their privacy, and they may suffer more cybercrimes as a result (Gross & Acquisti, 2005). Another

risk is that people tend to subscribe to multiple social media accounts, which may further increase privacy risks (de Paula, 2009).

Second, the pervasive personal privacy leakage of social media is exacerbated by exploding mobile computing usage because most of its users continually leak their locations in real-time to online social media—often without knowledge or consent (Keith et al., 2013). This newer phenomenon makes cyberstalking increasingly sophisticated and allows it to target victims in ways not possible in traditional stalking. New and "creepy" applications are being devised to exploit victims' privacy because of this new intersection of real-time location data and social media. To wit, Keith et al. (2013) recently illustrated an example involving i-Free's *Girls around Me* app (Mikhaylova, 2012), which led to its removal from the Apple App Store™, as they explain: "The app generated a map displaying the locations of single females in close proximity to the user. The availability of publicly shared personal and location data through the application programming interfaces (API) of Foursquare and Facebook allowed *Girls Around Me* to collect and display the names, personal photos, and most recent location(s) of single females. The fine line between "social networking app" and "creepy stalker app" was crossed by its "Make contact!" button, which facilitated the user's personal introduction to the female through the push notification feature of the female's Foursquare app." Similarly invasive apps are being continually envisioned and released, creating new rounds of unsuspecting victims, especially with a new series of apps that are explicitly designed for spying on boyfriends/girlfriends (Wealth Creation, 2013).

Third, the ubiquity and anonymity afforded by social media enable kinds of interpersonal relationships not seen in the real world. For example, research on relational behavior on Facebook has indicated that social media *facilitates* obsessive relational intrusion behavior

(Chaulk & Jones, 2011), such as obsession over ex-partners and harassment by ex-partners (Lyndon et al., 2011). Likewise, anonymity and distance allow people who would not engage in real-world stalking to engage in cyberstalking behaviors (Pittaro, 2007). Anonymous or fake identities make it much more difficult for law-enforcement agents to track down stalkers (Tavani, 2000) Likewise, true anonymity online allows for stalking opportunities that do not present themselves in the real world (Pittaro, 2007): anonymity allows people to seek revenge, make rude comments, post embarrassing pictures, and hurt people in ways not possible in the real world.

Fourth, cyberstalking departs from traditional stalking because it does not have to involve a series of repeated behaviors. Because information presented via social media "lives forever," one negative post or video can "live on" to create emotional trauma in a person, as if purposefully repeated acts by the initial offender were involved. A startling example is a recent case of "revenge porn" in which initial postings of nude photos from a jilted lover were almost immediately removed after the initial posting, but were reposted by others and spread to many servers over the years, and are still being reposted, thus causing so much trauma that the victim has felt "cyber raped," year after year (Miller, 2013). Notably, the postings of the photos by the jilted lover were not considered illegal, because they were initially taken under her consent and are considered his electronic property, which he is free to circulate under US guarantees of freedom of expression (or more precisely, under the lack of current laws dealing with the emergent phenomenon of "revenge porn"). Hence, such "cyber rape" is a legally protected behavior in many countries and jurisdictions because of the real-world legal vacuum surrounding the phenomenon. Stalking laws simply do not apply.

Fifth, online media allows for novel, pernicious cyberstalking behaviors that are not seen in the real world or come in unexpected forms, such as anonymous herds of bullies focusing on one victim, "revenge porn," virtual fake relationships, sending computer viruses as an act of revenge, modifying a photo of someone and reposting it to embarrasses him/her, and solicitation of minors for sexual purposes. Other examples of cyberstalking behaviors greatly modified from similar behaviors in the real world include online false accusations and threats, information theft, identity theft, electronic monitoring, and data damage for deviant social reasons (Bocij & McFarlane, 2002). Consequently, cyberstalking subsumes a rather wide variety of behaviors not normally associated with traditional stalking.

For example, although sexual solicitation of minors has long occurred, anonymity and identity cloaking have made social media the tool of choice for pedophiles, because they can more easily groom and ensnare countless victims who would not be susceptible in the real world (Dombrowski et al., 2004; Mitchell et al., 2007). In fact, youth Internet users are at most risk for the most serious forms of sexual solicitations (Mitchell et al., 2007).

Moreover, real-world stalking (e.g., Fox et al., 2009; Fox et al., 2011; McFarlane et al., 1999) and bullying (e.g., Nansel et al., 2001; Salmivalli et al., 1996) are traditionally studied separately as different behaviors by sociologists and psychologists. Traditionally, bullying was almost exclusively studied in terms of juvenile behavior and typically in the context of school (Nansel et al., 2001; Salmivalli et al., 1996). Meanwhile, such behaviors are so conflated online, and go well beyond juvenile behaviors, that cyberbullying is generally subsumed under cyberstalking or the terms are treated as interchangeable (Fukuchi, 2011), and cyberbullying/cyberstalking are now often studied together. Cyberbullying is an extension of real-world *bullying*, which can be defined as a repeated aggressive behavior to harm or disturb

victims in the context of an imbalance of power (Nansel et al., 2001). *Cyberbullying* can be defined as a deliberate, repeated, and hostile behavior to harm people anonymously through the Internet by leveraging the imbalance of power between bullies and victims (Kowalski et al., 2012; Smith et al., 2008).

Although the news media tends to focus on extreme cases of cyberbullying—such as those leading to suicide (Dahl, 2013; Huffingtonpost & Salazar, 2011; Neil Katz, 2010; Telegraph Reporters, 2013), rape (Neil Katz, 2010), sexual assault (Dahl, 2013), and abuse (Coyne, 2013)— cyberbullying can also involve less pernicious behaviors such as taunts and intimidation (Neil Katz, 2010), unwanted teasing, and implied threats. The most common forms of cyberbullying include forwarding private messages and spreading rumors (Claburn, 2007). Similarly, the US National Crime Prevention Council (National Crime Prevention Council, 2013) summarized common cyberbullying as online behaviors in which people "pretend they are other people to trick others, spread lies and rumors about victims, trick people into revealing personal information, send or forward mean text messages, and post pictures of victims without their consent."

Because of the many variations of cyberstalking, only a broad definition is possible at this point in the paper. Hence, we propose a general definition of *cyberstalking*, which builds on our definition of stalking, as one or more online postings or behaviors—motivated by an obsession with having power, control, and influence over a victim or multiple victims—that facilitate implicit and explicit threats, and thus induce fear in a victim. Our taxonomic work, presented in the next section, will further challenge and expand on this definition.

PROPOSING A TAXNOMY AND EXPANDED DEFINITION OF CYBERSTALKING

Again, new areas of theoretical development can progress adequately only with proper nomenclature for and taxonomies of the phenomenon involved (Lowry et al., 2004; Posey et al., 2013). Thus, a taxonomy of the facets of cyberstalking is required in order to explain and predict the phenomenon more effectively. In this section, we first review existing classifications of cyberstalking/cyberstalkers, and then propose a two-dimension taxonomy of cyberstalking behaviors. We then refine our proposed definition of cyberstalking.

Several attempts at taxonomies or more elaborate definitions of cyberstalking have been made in the literature. Although the motivations of stalkers as well as the relationship between stalkers and victims are widely discussed in cyberstalking research, no common nomenclature or taxonomy has been produced.

Behavioral Patterns of Cyberstalkers

The first criterion of our taxonomy, the behavioral patterns of cyberstalkers, focuses on illustrating how and to what extent a cyberstalker gains access to and interacts with the victim. Again, due to the enormous overlap between cyberstalking and cyberbullying, some of these categories are more commonly recognized as cyberbullying; again, however, we do not further distinguish these, as the motivations are largely the same. Based on our comprehensive review of the literature and real-world cyberstalking cases, we propose three major types of behavioral patterns adopted by cyberstalkers: (1) cyberstalking in secret, (2) indirect cyberstalking, and (3) direct cyberstalking. Table 3 expands these into nine variations or subtypes.

Motivations of Cyberstalkers

The second criterion of our taxonomy, the motivations of cyberstalkers, focuses on illustrating why the stalking behavior is performed. Based on the various stalking motivations listed in the relevant studies (Bocij, 2004; Bocij et al., 2002; Bocij & McFarlane, 2002; Bocij & McFarlane, 2003; QuitStalkingMe, 2011; SAPAC, 2013) and the many behaviors we observed in the literature, we further summarize and reclassify the stalking motivations into four groups:

(1) To fulfill cyberstalkers' psychological needs, wishes, or cravings regarding another person (e.g., obsessive curiosity about someone, wanting to make fun of someone, venting a bad mood gratuitously)

(2) To instill fear in or gain control over a victim

(3) To seek revenge or punish the victim (usually resulting from negative emotions toward the victim, such as anger and jealousy)

(4) To build a relationship with the victim (including sexual relationships or those acting out a fantasy)

Although we categorize each of our example behaviors according to a single motivation, we recognize that a cyberstalker can have more than one motivation. However, for simplicity, we categorize each behavior in view of its most probable primary motivation.

Toward an Expanded Definition of Cyberstalking

Given the real-world and research examples of actual behaviors and motivations of cyberstalking, we believe our improved taxonomy improves the understanding of cyberstalking itself and indicates why it is not a merely a form of traditional stalking. In particular, our two added dimensions, to the extent that they hold for all cyberstalking cases, lead us to refine our

definition of cyberstalking as follows: *cyberstalking* involves one online behavior or a series of online behaviors that is/are (1) secret, (2) indirect, or (3) direct, targeted toward another person, group, or organization, and motivated by a stalker's desire to (1) fulfill psychological needs, wishes, or cravings regarding another person; (2) to instill fear in a victim or to gain control over a victim; (3) to seek revenge or punish the victim; or (4) to build a relationship with a victim.

PROPOSING A THEORETICAL MODEL OF CYBERSTALKING

This section begins with a review of theories that can be used to explain cyberstalking. Our taxonomy highlights that cyberstalkers can have a number of motivations, which motivations greatly outnumber the more limited set found in traditional stalking. Thus, a useful theoretical model of cyberstalking needs to account reasonably for these possible motivations. To do so systematically, we reviewed a wide number of theories of the *intrapersonal*, *situational*, and *interpersonal* levels that most likely encompass these motivations. Based on this critical review, we propose a theoretical model of cyberstalking based on the five theories from this review that we identify as the most efficacious in explaining cyberstalking. First, three theories are selected for the intrapersonal level: the emotional theory of stalking (Spitzberg, 2000), neutralization theory (Sykes

&Matza, 1957), and the self-control theory of crime (Gottfredson & Hirschi, 1990). Second, we use rational choice theory (Becker, 1968) as a broad theory for situational-based decision making. Third, for our interpersonal theory, we leverage the social learning theory of crime (Akers, 1973).

INTRAPERSONAL-LEVEL THEORIES EXPLAINING CYBERSTALKING

Theories at this level typically emphasize the cognitive and emotional factors that affect outcomes within a person or occurring within one's mind. The theories, on this level, that we believe are relevant to cyberstalking include the emotional theory of stalking, the neutralization theory, and the self-control theory of crime.

Emotional Theory of Stalking and Cyberstalking

In developing the emotional theory of stalking, Spitzberg (2000) pointed out two negative emotions that deserve attention: shame and anger. These emotions can contribute to explaining the emotional mechanism of cyberstalking. Anger can be the catalyst that encourages a person to cyberstalk (e.g., for revenge). Because most cyberstalking behaviors violate social norms, a cyberstalker is likely to experience shame both before and after the cyberstalking behavior, and possibly because of high levels of anger itself. Following this line of reasoning, because we are focused on the predictors as opposed to the results of cyberstalking, shame is particularly useful in our theoretical model.

Shame can be invoked in two major ways: by breaking a moral code or by being put in a negative social light. Either form of shame should decrease cyberstalking. To experience guilt-induced shame, one must have an underlying moral or ethical code that they transgress, and this transgression facilitates the guilt needed for this form of shame to occur (Spitzberg, 2000; Tangney et al., 1996). Morality and shame and thus intertwined (Lamb, 1983), though shame is a broader concept than moral guilt. It is possible to experience shame for factors outside of from transgressing a moral code, such as something in general reflecting negatively about one's identity (e.g., unflattering photo) (Olthof et al., 2004).

If potential cyberstalkers believe that cyberstalking actions will violate moral codes, they are likely to feel guilt and subsequent shame; such uncomfortable feelings will make them less likely to cyberstalk others. Likewise, if potential cyberstalkers feel cyberstalking could put themselves in a negative light in which they would experience shame, they are less likely to cyberstalk. For example, IT literature shows that people with strong moral or ethical dispositions are less likely to commit purposeful security violations (Myyry et al., 2009) or are more likely to adopt anti-plagiarism software (Lee, 2011). More recently, Siponen et al. (2012) explain moral beliefs, with its associated guilt and shame production, as a key catalyst in preventing software piracy. As an important limitation to the scope of this theory is that it does not apply well to sociopaths. Sociopaths are people who suffers from psychopathy, in which they are abnormally immune to the influence of morality and ethics in their behaviors, among other personality disorders (Koenigs et al., 2011; Young et al., 2012).

Neutralization Theory and Cyberstalking

Originating in criminological research, neutralization theory has been widely used in explaining delinquent behavior. One of the basic assumptions of neutralization theory is that people who engage in delinquent behavior also "believe in the norms and values of the community in general" (Siponen & Vance, 2010, p. 489). Earlier studies had proposed that there is a distinction between "acts that are wrong in themselves" and "acts that are illegal but not immoral" (Sykes & Matza, 1957, p. 667): the former will cause significantly more guilt in the delinquents than the latter.

Therefore, non-sociopathic people feel guilty and ashamed when they realize that their own behaviors do not comply with established moral standards, which in turn prevents them

from performing illegal and improper behaviors. However, before engaging in delinquent behavior, delinquents tend to justify such behavior subjectively, and certain neutralization techniques help them to justify their delinquent behaviors as moral and proper.

Siponen and Vance (2010) further adopted neutralization theory to explain law-abiding and rule-breaking actions using IT in organizations. Their empirical study additionally supported the argument that a set of neutralization techniques outlined in the criminology literature helps employees to rationalize their rule-breaking behaviors in the IS context. Although neutralization theory is not yet widely used in the IS field, similar perspectives have been used to explain the problematic use of information systems. For instance, Harrington (1996) argued that by denying responsibility for the potential consequences, employees are more likely to perform computer abuse behavior. In addition, Puhakainen (2006) found that employees sometimes failed to comply with rules requiring the encryption of confidential emails because they thought the company was at fault for failing to make the rules clear. From the standpoint of these studies, people use certain techniques to persuade themselves that some of the deviant behaviors they want to perform are actually reasonable, and this process contributes significantly to their eventual actions. Following the research of Siponen and Vance (2010), Gregory and Brekashvili (2012) adopted neutralization theory to understand employees' whistleblowing intentions, while Li and Cheng (2013) combined neutralization theory with rational choice theory to propose that neutralization techniques contribute significantly to Internet abuse in the workplace. To summarize, these studies have indicated that neutralization theory can be applied to explain problematic and delinquent behavior in the cyberworld context, especially when the risk to the offender is relatively low (Li & Cheng, 2013).

Examples of neutralization techniques used by delinquents to justify their behaviors include denial of responsibility, denial of injury, denial of the victim, condemnation of the condemners, appeal to higher loyalties (Sykes & Matza, 1957), the metaphor of the ledger (Klockars, 1974), and the defense of necessity (Minor, 1981). Table 4 summarizes the relevant neutralization techniques examined in previous studies and offers corresponding examples of neutralization techniques that could be used to justify cyberstalking.

Before performing a cyberstalking behavior, it is likely that cyberstalkers will engage in multiple neutralization techniques to justify their behavior. Which ones they choose is not as theoretically important for our model as the key proposition is that they will engage in neutralization as a key facilitator of cyberstalking. Under this assumption, when cyberstalkers attempt to justify their delinquent behavior, they will adopt a certain combination of these techniques to realize the overall neutralizing effect at which they aim.

One of the basic assumptions of neutralization theory is that moral beliefs serve as obstacles to performing delinquent behavior (Siponen et al., 2012). Similarly, several security-related studies in IS outside of neutralization identify morality as an information sanction or impediment against inappropriate online security-related and piracy behaviors. (Lee, 2011; Myyry et al., 2009; Vance & Siponen, 2012). Neutralization then serves as a psychosocial method to overcome such psychological obstacles: using multiple techniques of neutralization, cyberstalkers will diminish their sense of guilt and shame and ultimately facilitate their cyberstalking. In addition to this indirect relationship, metaphor of the ledger help cyberstalkers claim that it is “just” and their “proper right” to cyberstalk others, which directly increases the cyberstalking. If this is the case, then a more moral person is less likely to succumb to neutralization.

Self-Control Theory of Crime and Cyberstalking

The final intrapersonal theory we leverage is the general theory of crime, also called the self-control theory of crime, which argues that individuals with low self-control are more likely to commit crime when presented with the opportunity (Gottfredson & Hirschi, 1990). Gottfredson and Hirschi (1990) did not provide a clear operational definition of self-control, they simply used *low self-control* and *high self-control* "as labels for this differential propensity to commit crime" (Akers, 1991, p. 204). Specifically, risk seeking, impulsivity, a temperamental personality, shortsightedness, self-centeredness, and a preference for physical activities are regarded as six traits representing low self-control. People with these traits will have a lower degree of self-control and therefore a stronger inclination to engage in criminal actions.

Self-control theory is widely used to understand various criminal behaviors, including academic cheating (Bolin, 2004), fraud (Holtfreter et al., 2008), date violence (Schreck et al., 2008), theft (Schreck, 1999), and the like. Tibbetts and Gibson (2002) suggested that low self-control is one of the most important factors influencing criminal decision making. Fox et al. (2009) first applied self-control theory in the context of stalking and suggested that low self-control is related to both stalking behaviors and stalking victimization; its relationship to stalking victimization was significant only among women. Bossler and Holt (2010) further proposed that self-control theory can be expanded to explain cyberworld victimization and that low self-control contributes significantly to cyberworld victimization under low-risk situations. Similarly, to understand information security policy violation, Hu et al. (2011) integrated self-control with other rational choice factors in their research. In view of these studies, it is useful to adopt self-control theory in the context of cyberstalking.

According to self-control theory, people with a low degree of self-control are less able to control their emotions and behaviors and thus are more inclined to seek immediate gratification. The personal trait of low self-control makes them more emotion-driven and directly forms the intention to perform delinquent behavior regardless of other rational considerations. Thus, they are more likely to have a higher degree of cyberstalking as "an efficient and effective means to satisfy immediate gratification" (Bossler & Holt, 2010, p. 228).

SITUATIONAL-LEVEL THEORIES EXPLAINING CYBERSTALKING

Theories on the situational level are designed to account for the situational factors of the external environment, such as economic, social, or IT factors. Different theories provide different explanations for how these factors facilitate negative behaviors such as stalking. For example, *routine activities theory* concentrates on the circumstances in which criminals carry out predatory criminal acts. This theory emphasizes that most criminal acts require the convergence in space and time of likely offenders, suitable targets, and the absence of capable guardians against crime (Cohen & Felson, 1979). Holt and Bossler (2008) applied routine activities theory to the empirical study of cyberstalking; they found that individual and peer involvement also significantly increased the risk of victimization in computer crime and deviance. Reyns et al. (2011) developed an adapted lifestyle–routine activities theory specifically for the cyberstalking context; they distinguished many significant predictors, including exposure to risk, online proximity, online guardianship, and online deviance. However, as these studies have illustrated, the use of routine activities theory in cyberstalking best focuses on the perspective of the victim rather than that of the stalker; therefore, it is not

appropriate for explaining the internal mechanisms of cyberstalking behavior under investigation here.

As a more promising theory, Becker (1968) initially introduced *rational choice theory* (RCT) into the literature as an extended economic approach to crime. Drawing upon economic, political, and sociological research, the rational choice approach assumes that individuals, on the microeconomic level, analyze and plan to make reasoned decisions for a given situation or context (McCarthy, 2002). RCT argues that, in the process of rational decision making, people primarily identify alternative actions and the likely outcomes of each (Bulgurcu et al., 2010). The rationality is determined by balancing the costs against the benefits of one's actions to maximize personal advantage. The calculus of perceived expectations not only refers to material goods, but also includes a vast array of outcomes (McCarthy, 2002). Hence, the decision to perform a criminal behavior represents an overall assessment of costs and benefits shaped by an individual's perception of the criminal action (Bulgurcu et al., 2010). Because of its economic contributions and the empirical reality of crime, the RCT approach has been widely used in criminology research in conjunction with other theoretical frameworks, such as those emphasizing moral beliefs, deterrence, and self-control (Hu et al., 2011).

General deterrence theory (GDT) is also a well-established theory in criminology; it posits that deviant behaviors could be deterred by the administration of disincentives and sanctions relevant to the deviance (Ehrlich, 1973). The key assumption of GDT is that specific punishments will prevent offenders from committing the crimes and that the response to punishment (e.g., fear) will prevent others from committing similar crimes (Gottfredson & Hirschi, 1990). This assumption is the basis for the two central tenets of GDT: *certainty of*

sanctioning and *severity of sanctioning* (Blumstein et al., 1978). According to GDT, organizations can predict the offender's behavior by assessing the two dimensions of sanctions and inhibiting the deviant behavior by administrative disincentives.

Like RCT, GDT takes into account some of the costs of deviant behavior. However, GDT focuses exclusively on the sanctions of deviant behavior, which focus is too narrow to explain a lot of cyberstalking phenomenon. Although the punishments or disincentives can be viewed as the cost of deviant behavior, some cyberstalking that is harmful to the victims (e.g., searching private information without permission) may not be sensed, especially because anonymity is a major facilitating factor; therefore, it is not easily prevented by traditional sanctions. Furthermore, because anonymity can cloak cyberstalkers' identities, the risk of sanctions is much lower in cyberstalking than real-world stalking. Because RCT considers both the benefits and costs of deviant behavior, we believe it is more appropriate than GDT for explaining cyberstalking behavior.

Another advantage of adopting RCT is that it can be used to complement neutralization theory. Neutralization theory explains the rationalizations used by cyberstalkers, but RCT can better explain the motivations of cyberstalking. If this is true, the intention that accrues to the individual from cyberstalking is partially or largely influenced by the individual's perception of the costs and benefits of potential outcomes. Thus, we use RCT to identify those cyberstalking-related consequences—the rational calculus of the costs and the benefits. In our context, the outcomes of an individual's stalking behavior are the contemplation of costs (e.g., risks and punishment) and benefits (e.g., accomplishment and materials) of the associated action. We define the *perceived benefit* of cyberstalking as the overall expected favorable consequences for an individual engaging in cyberstalking, whereas the *perceived cost* of

cyberstalking is defined as the overall expected unfavorable consequences (Bulgurcu et al., 2010).

Following Bulgurcu et al. (2010) and Hu et al. (2011), we include perceived extrinsic and intrinsic benefits as the favored consequences of cyberstalking. *Perceived extrinsic benefits* refer to the material benefits (e.g., rewards) as external motivations for cyberstalking. Conversely, *perceived intrinsic benefits* are an individual's intrinsic motivations—such as the contentment, satisfaction, accomplishment, and fulfillment derived from cyberstalking itself—to cyberstalk someone in social media (Bulgurcu et al., 2010).

Previous studies have also recognized that the risk of getting caught will deter individuals from committing crimes (Siponen & Vance, 2010). This cognitive characteristic of individuals will affect how the costs of desired actions are perceived (Hu et al., 2011). Obviously, "opportunities linked to a low risk of being caught" are less costly and more favorable than the "opportunities linked to a high risk" (Seipel & Eifler, 2010, p.173). Importantly, although perceived risk will decrease cyberstalking, because of greater anonymity, social distance, and fewer legal controls, the risks of cyberstalking will frequently be seen as lower than those of traditional stalking. Nonetheless, from an RCT perspective these potential risks and costs can be represented in terms of intrinsic costs (Bulgurcu et al., 2010), formal sanctions (severity and certainty) (Bulgurcu et al., 2010), and informal sanctions (Vance & Siponen, 2012). We omit intrinsic costs, because these include guilt, embarrassment, and shame (Bulgurcu et al., 2010), which are already sufficiently represented in our model. However, we include informal sanctions, which include the idea of guilt but adds the important elements of social disapproval from friends and peers. Summarizing this section, we propose:

Moderation Effects of Self-Control on Cyberstalking

Finally, in our model, we discuss the possible moderating effects of low self-control. We add this possibility because a significant amount of the literature has discussed the relationship between self-control and rational thinking (Baron et al., 2007; Bossler & Holt, 2010; Fox et al., 2009; Hu et al., 2011; Piquero & Tibbetts, 1996; Seipel & Eifler, 2010). According to these studies, self-control not only serves as an alternative factor of rational choice measures that have a direct influence on the intention to perform delinquent behavior, but it also moderates the relationship between rational choice factors and the behavioral intention. Individuals with low self-control are less likely to calculate the risk and benefit involved in their real-world stalking behavior (Fox et al., 2009), and this is likely in cyberstalking, as well. That is, those with low self-control are simply less, rational in general. They do things more out of impulse then out of cost-benefit considerations.

INTERPERSONAL-LEVEL THEORIES EXPLAINING CYBERSTALKING

Theories on the interpersonal level usually consider the influence of social relations. The social experience of stalkers as well as their interaction within their social network would certainly be useful in understanding cyberstalking. In particular, *social learning theory* posits that crime is a social behavior learned largely by interacting within intimate groups (e.g., peers); that is, a criminal or delinquent actor models and imitates the deviant behavior of fellow group members.

We adopt the social learning theory in the context of cyberstalking for several reasons. First, although social learning theory is widely used as a general theory to explain most deviant

behaviors, it was originally designed by Akers (1973) and Bandura (1977) to explain offending and related behavior, which is indeed consistent with our context.

Second, previous studies have already adopted social learning theory to explain general stalking behaviors. Fox et al. (2011), for instance, applied it to examine the social factors related to stalking and concluded that the four explanatory variables of social learning theory are important predictors of both stalking perpetration and victimization.

Third, social learning theory has been shown to be effective not only in understanding traditional deviant and criminal behavior, but also in understanding deviant and criminal behavior occurring in the cyberworld context—for instance, in general criminal computer behavior (Rogers, 2001; Skinner & Fream, 1997), software piracy (Higgins, 2006; Higgins & Makin, 2004), and computer abuse within organizations (Lee & Lee, 2002). All these studies have provided theoretical and empirical evidence that various deviant and criminal actions in the cyberworld are, like their real-world counterparts, partially learned from social interactions.

Finally, the social media context of this study is highly social and interactive by its very nature; social media fuels such social interactions and mimicking behaviors. Given the importance of social influence and interaction in social media, it is natural to expect that a social learning process can have an important influence on individual cyberstalking behavior. This is particularly true in mimetic behavior, such as group bullying and insulting posts. In fact, we may be witnessing a social shift in which much traditional socialization is now learned by children and adolescents online (O'Keeffe et al., 2011).

As a general theory explaining criminal behaviors, social learning theory was built on the differential association-reinforcement theory (Burgess & Akers, 1966) and later further developed by Akers (1973), who introduced alternative variables such as definitions and imitation. Therefore, it maintains a comprehensive perspective (Rogers, 2001). There is a significant amount of discussion in the literature where its overlaps with RCT (Akers, 1990) and interacts with self-control theory (Higgins, 2006; Higgins & Makin, 2004). Because we focus specifically on how the social interaction process within intimate groups influences the behavioral patterns of cyberstalkers, in this section we adopt differential association as the most relevant variable from the interpersonal level and omit the overlapping elements in order to reflect the influence of social interaction with peers.

The other three variables from the social learning theory—differential reinforcement, definitions, and imitation—are excluded for the following reasons. First, although they all reflect the key idea of social learning theory that deviant behaviors are learned within the social interaction process, they overlap significantly with theories from the intrapersonal level (i.e., neutralization theory and self-control theory) and situational level (i.e., rational choice theory), and do not belong exclusively to the interpersonal level. For instance, differential reinforcement is highly similar to RCT variables (i.e., benefits and punishments), which construe deviant behaviors from an economic perspective, whereas definitions, which reflect the inner attitudes and beliefs of stalkers, will further influence the neutralization process.

Second, while discussing the interrelationships among the four social learning variables, Akers et al. (1979) claimed that differential association occurs first in the social learning process and that the other three variables largely depend on it. Consequently, differential association is pivotal and foundational. Without it, it is meaningless to discuss the reinforcement and imitation process or how definitions are formed in the minds of individuals.

Third, with respect to the social learning theory, the variable of definitions emphasizes the inner moral value formed from past experiences that may further influence the use of neutralization techniques, whereas differential reinforcement and imitation describe how past experience will influence the perceived benefits and risks. Thus, definitions, differential reinforcement, and imitation have a less direct influence on determining a deviant behavior in a specific situation. As a result, their influence has been frequently insignificant in empirical studies (Skinner & Fream, 1997). Thus, for theoretical parsimony, we adopt differential association as the most relevant variable from social learning theory and exclude the other three.

Differential association attempts to capture the extent to which individuals are exposed to deviant behavior through their association with others. According to social learning theory, deviant behaviors are learned from models that emerge in social interactions. Thus, individuals who are more frequently exposed to cyberstalking behaviors are more likely to learn to cyberstalk others. In contrast, individuals who are less frequently exposed to cyberstalking behaviors are less likely to form the motives and habits to cyberstalk others or to gain the skills necessary to do so.

DISCUSSION

Although stalking is widely studied in the traditional offline context, few comprehensive studies and theories explain and predict stalking behavior in the cyberworld context. The problem is due partly to the divergent conceptualizations and taxonomies of cyberstalking. Our study thus starts by proposing a common nomenclature for and taxonomy

of cyberstalking, which can be used by researchers and practitioners to better understand its differences from traditional stalking. We then propose a meaningful theoretical model that captures, and can explain and predict, the most likely motivations and behaviors involved in cyberstalking. Our model integrates five theories within three levels: the intrapersonal level (emotional theory, neutralization theory, and self-control theory), the situational level (rational choice theory), and the interpersonal level (social learning theory).

Although our model integrates five theories, we believe that neutralization theory forms the foundation of our model, and that the other theories provide additional explanation. We suggest that neutralization theory can be used to explore cyberstalking and that it is appropriate for our context of social media for several reasons. First, neutralization theory fits the context of cyberstalking well. Although cyberstalking is generally regarded as deviant behavior and usually inflicts harm on the victim, the motivation of cyberstalkers is not always purely negative. For instance, sometimes they cyberstalk others out of curiosity and admiration, and even because they want to build a relationship with the victim (albeit often in a misguided approach). Moreover, with the development of Internet tools and social media, cyberstalking has become widespread. Consequently, to the extent cyberstalkers feel any degree remorse, shame, or moral reservations in their behavior, neutralization techniques help them overcome their reservations against cyberstalking.

Second, compared with other theories, neutralization theory can be generalized effectively to cyberstalking behavior and is particularly illuminating in the low-risk contexts of social media. According to Seipel and Eifler (2010), when rational choice theory is used to explain individual behavior, it has strong explanatory power for high-cost situations. Only when the cost is sufficiently high will the delinquent seriously calculate the costs and benefits

to decide whether to perform delinquent behaviors. In contrast, neutralization theory describes techniques used to overcome moral constraints rather than to lower the risks of being punished. In terms of the context of this study, most cyberstalking cases do not constitute crimes, and certain technological affordances of the Internet, such as the high degree of anonymity and virtual identities, make it difficult for cyberstalkers to be punished or socially censured. Hence, cyberstalking is generally much less risky to the perpetrator than real-world stalking. Because neutralization theory focuses on moral constraints instead of personal risk, it thus represents an effective tool for explaining deviant behaviors in the relatively low-risk context of cyberstalking.

Third, although neutralization theory has been applied primarily in organizational contexts in previous IS literature (Gregory & Brekashvili, 2012; Harrington, 1996; Li & Cheng, 2013; Puhakainen & Ahonen, 2006; Siponen & Vance, 2010), we believe it can be used more convincingly to explain individual behaviors in the general social environment. Derived from criminology to explain individual deviant behavior, neutralization theory helps to clarify how deviants view their illegal behaviors as morally correct by using their delinquent subculture to distort the generally accepted culture (Sykes & Matza, 1957). In organizational studies, if the mainstream organizational culture's policies and rules are not widely known and not accepted by employees, they do not need the neutralization process to break them. However, in the cyberworld and social media context, the general cultures' real-world moral rules are widely known and, to some degree, still effective in regulating netizens' behavior. We also argue that deviant behavior at work is far more risky that deviant (often anonymous) behavior online. Hence, we believe that neutralization applies even more strongly to cyberstalking than in organizational settings.

Nonetheless, the other theories we isolated—the emotional theory of stalking, self-control theory, rational choice theory, and social learning theory—provide important additional explanations of cyberstalking. The theories from the intrapersonal level (the emotional theory of stalking and self-control theory) provide explanatory variables such as neutralization, shame, and self-control to reflect the impact of mental activities, inner perceptions, and personality traits on cyberstalking. Using explanatory variables such as perceived benefits and risks, rational choice theory, as a situational-level theory, helps to predict the cyberstalking based on specific situations. Finally, as an interpersonal-level theory, social learning theory emphasizes how interactions with the social environment influence individual cyberstalking behavior. By integrating all these explanatory variables into a coherent model, we can now better understand how to explain and predict cyberstalking behaviors.

In closing, aside from empirically testing our model, several more theoretical possibilities remain. For one, the model could be expanded to consider cyberstalking continuance. Like other continuance models, the roles of habit or even addiction can come into play. Habit formation derives from positive feedback loops of positive emotional arousal from a specific behavior, and in systems use has been shown to link to continuance in (Khalifa & Liu, 2007). (Limayem et al., 2007; Polites & Karahanna, 2013). Positive feedback experiences in cyberstalking could thus lead to habit in cyberstalking, or to cyberstalking continuance. Such phenomenon would thus help explain people who keep cyberstalking even when they get caught, such as the famous case of Anthony Weiner's multiple sexting scandals (Anonymous, 2013a).

The role of sociopathy in cyberstalking also introduces intriguing possibilities: To include sociopaths, the model would need to contextually drop morality, shame, and guilt when a sociopath is involved because they are generally immune to these emotions when making

behavioral decisions (Koenigs et al., 2011; Young et al., 2012). Neutralization and RCT would likely play a stronger role for sociopaths than people with a degree of moral conscience. Certainly, theoretical development and empirical research on cyberstalking has many exciting and intriguing possibilities.

REFERENCES

ACLU. (2013). *Warrantless cell phone location tracking*. Retrieved September 9, 2018, from https://www.aclu.org/technology-and-liberty/warrantless-cell-phone-location-tracking

Adam, A. (2002), "Cyberstalking and internet pornography: Gender and the gaze," *Ethics and Information Technology* 4(2), pp. 133-142.

Akers, R. L. (1973). *Deviant Behavior: A Social Learning Approach*. Belmont, CA: Wadsworth.

Akers, R. L. (1990), "Rational choice, deterrence, and social learning theory in criminology: The path not taken," *The Journal of Criminal Law & Criminology* 81(3), pp. 653-676.

Akers, R. L. (1991), "Self-control as a general theory of crime," *Journal of Quantitative Criminology* 7(2), pp. 201-211.

Akers, R. L., Krohn, M. D., Lanza-Kaduce, L., & Radosevich, M. (1979), "Social learning and deviant behavior: A specific test of a general theory," *American Sociological Review* 44(4), pp. 636-655.

Alexy, E. M., Burgess, A. W., Baker, T., & Smoyak, S. A. (2005), "Perceptions of cyberstalking among college students," *Brief Treatment and Crisis Intervention* 5(3), pp. 279-289.

Anonymous. (1999). *Man charged in California cyberstalking case*. Retrieved September 19, 2018, from http://www.history.com/this-day-in-history/man-charged-in-california-cyberstalking-case

Anonymous. (2010). *A friend request from who?* Retrieved September 8, 2018, from http://www.gobigsocialmedia.com/a-friend-request-from-who/

Anonymous. (2013a). "Anthony Weiner sexting scandals," Retrieved September 20, 2013, from http://en.wikipedia.org/wiki/Anthony_Weiner_sexting_scandals

Anonymous. (2013b). *Man sends Facebook friend request to female coworker-Suspended from work for sexual harassment* Retrieved September 8, 2018, from http://www.muripo.com/2013/07/24/man-sends-facebook-friend-request-to-female-coworker-%E2%86%92-suspended-from-the-office-for-sexual-harassment/

Arnold, B. (2008). *Online and offline stalking incidents and prosecutions*. Retrieved September 8, 2018, from http://www.caslon.com.au/stalkingnote4.htm

Bandura, A. (1977). *Social Learning Theory*. Englewood Cliffs, NJ: Prentice-Hall.

Bandura, A. (1999), "Moral disengagement in the perpetration of inhumanities," *Personality and Social Psychology Review* 3(3), pp. 193-209.

Baron, S. W., Forde, D. R., & Kay, F. M. (2007), "Self-control, risky lifestyles, and situation: The role of opportunity and context in the general theory," *Journal of Criminal Justice* 35(2), pp. 119-136.

Basu, S. & Jones, R. (2007), "Regulating cyberstalking," *Journal of Information, Law and Technology* 2(1), pp. 1-30.

Baum, K., Catalano, S., Rand, M., & Rose, K. (2009). *Stalking Victimization in the United States*. Washington, DC: US: Department of Justice, National Institute of Justice.

Beal, M. (2005). *Internet facilitates celebrity stalking*. Retrieved September 14, 2018, from http://www.theeagleonline.com/article/2005/10/internet-facilitates-celebrity-stalking

Becker, G. S. (1968), "Crime and punishment: An economic approach," *Journal of Political Economy* 76(2), pp. 169-217.

Blumstein, A., Cohen, J., & Nagin, D. (1978). *Deterrence and Incapacitation: Estimating the Effects of Criminal Sanctions on Crime Rates*. Washington, DC: National Academy of Sciences

Bocij, P. (2002), "Corporate cyberstalking: An invitation to build theory," *First Monday* 7(11).

Bocij, P. (2004). *Cyberstalking: Harassment in the Internet Age and How to Protect Your Family*. Westport, CT: Praeger Publishers.

Bocij, P., Griffiths, M., & McFarlane, L. (2002), "Cyberstalking: A new challenge for criminal law," *Criminal Lawyer* 122(3), pp. 3-5.

Bocij, P. & McFarlane, L. (2002). Online harassment: Towards a definition of cyberstalking. *Prison Service Journal*, *139*, 31-38.

Bocij, P. & McFarlane, L. (2003), "Cyberstalking: The technology of hate," *The Police Journal* 76(3), pp. 204 -221.

Bolin, A. U. (2004), "Self-control, perceived opportunity, and attitudes as predictors of academic dishonesty," *The Journal of Psychology* 138(2), pp. 101-114.

Boon, J. & Sheridan, L. (2002). *Stalking and Psychosexual Obsession: Psychological Perspectives for Prevention, Policing and Treatment*. New York,NY: John Wiley & Sons.

Bosker, B. (2010). *Ugly Meter iPhone App Raises Cyberbullying Concerns* Retrieved 14 Sept, 2018, from http://www.huffingtonpost.com/2010/10/20/ugly-meter-iphone-app-rai_n_769471.html

Bossler, A. M. & Holt, T. J. (2010), "The effect of self-control on victimization in the cyberworld," *Journal of Criminal Justice* 38(3), pp. 227-236.

Brownlee, J. (2012). *Creepy girl-stalking app girls around me has been yanked from the app store*. Retrieved September 19, 2018, from http://www.cultofmac.com/157918/creepy-girl-stalking-app-girls-around-me-has-been-yanked-from-the-app-store/

Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010), "Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness," *MIS Quarterly* 34(3), pp. 523-548.

Bully Online. (2013). *Bullying: what is it? Types of bullying, bullying tactics, how targets are selected, the difference between bullying and harassment—An answer to the question "Why me?"*. Retrieved September 8, 2013, from http://www.bullyonline.org/workbully/bully.htm

Burgess, R. L. & Akers, R. L. (1966), "A differential association-reinforcement theory of criminal behavior," *Social Problems* 14(2), pp. 128-147.

Campbell, D. (2012). *Infatuated patients use Facebook to stalk doctors*. Retrieved July 29, 2013, from http://www.guardian.co.uk/society/2012/oct/28/lovesick-patients-stalk-doctors-online

Canadian Civil Liberties Association. (2012). *Supreme court releases decision in the 'fake Facebook' case*. Retrieved Sept 19, 2013, from http://ccla.org/2012/09/27/Supreme-Court-Releases-Decision-in-Fake-Facebook-Case/

Cavalier, C. (2013). *What to do when someone corrects your grammar*. Retrieved September 8, 2013, from http://www.purplecar.net/2013/09/grammar-bullies/

Chao, C.-H. (2011). Reconceptualizing the mechanism of Internet human flesh search: A review of the literature, *2011 International Conference on Advances in Social Networks Analysis and Mining (ASONAM)* (pp. 650-655). Kaohsiung, Taiwan: IEEE.

Chaulk, K. & Jones, T. (2011), "Online obsessive relational intrusion: Further concerns about Facebook," *Journal of Family Violence* 26(4), pp. 245-254.

Citron, D. K. (2009), "Cyber civil rights," *Boston University Law Review* 89(61), pp. 61-125.

Claburn, T. (2007). *Cyberbullying common, more so at Facebook and MySpace*. Retrieved September 8, 2013, from http://www.informationweek.com/cyberbullying-common-more-so-at-facebook/200001167?cid=tab_art_sec#community

Cluley, G. (2013). *Hackers attack games publisher Ubisoft, steal players' personal information*. Retrieved September 14, 2013, from http://grahamcluley.com/2013/07/ubisoft-hack/

Cohen, L. E. & Felson, M. (1979), "Social change and crime rate trends: A routine activity approach," *American Sociological Review* 44(4), pp. 588-608.

Costa, C. (2012). *Are you a cyberstalker? Shocking statistics say yes*. Retrieved July 29, 2013, from

http://hightechrealm.com/2012/11/are-you-a-cyberstalker-shocking-statistics-say-yes/

Coyne, E. (2013). *Cyberbullying websites should be boycotted, says Cameron*. Retrieved September 12, 2013, from http://www.theguardian.com/society/2013/aug/08/cyberbullying-websites-boycotted-david-cameron

Cromwell, P. & Thurman, Q. (2003), "The devil made me do it: Use of neutralizations by shoplifters," *Deviant Behavior* 24(6), pp. 535-550.

Cross, D. (2009). *Australian covert bullying prevalence study*. Perth: Child Health Promotion Research Centre, Edith Cowan University.

Cupach, W. R. & Spitzberg, B. H. (2004). *The Dark Side of Relationship Pursuit: From Attraction to Obsession and Stalking*. Mahwah, NJ: Routledge.

Cyber Law. (2012). *How to beat cyber stalkers at their own game* Retrieved September 19, 2018, from http://riverdelfin.blogspot.hk/2013/06/how-to-beat-cyber-stalkers-at-their-own.html

D'Arcy, J. & Herath, T. (2011), "A review and analysis of deterrence theory in the IS security literature: making sense of the disparate findings," *European Journal of Information Systems* 20(6), pp. 643-658.

D'Ovidio, R. & Doyle, J. (2003), "A study on cyberstalking: Understanding investigative hurdles," *FBI Law Enforcement Bulletin* 72(3), pp. 10-17.

Dahl, J. (2013). *Audrie Pott, Rehtaeh Parsons suicides show sexual cyber-bulling is "pervasive" and "getting worse*," expert says. Retrieved September 8, 2013, from http://www.cbsnews.com/8301-504083_162-57579366-504083/audrie-pott-rehtaeh-parsons-suicides-show-sexual-cyber-bulling-is-pervasive-and-getting-worse-expert-says/

Daily Mail Reporter. (2009). *'Chilling' cyber stalker terrorised girl with Facebook death threats for two years after she refused to go out with him*. Retrieved September 19, 2018, from http://www.dailymail.co.uk/news/article-1226349/Chilling-cyber-stalker-terrorised-girl-Facebook-death-threats-years-refused-him.html

Day, T. R. (2010). "The new digitial dating behavior-sexting: Teens' explicit love letters: Criminal justice or civil liability," *Express*. Retrieved September 20, 2018, from http://works.bepress.com/terri_day/6

de Paula, A. M. (2009). Security aspects and future trends of social networks, *Proceedings of The Fourth International Conference on Forensic Computer Science (ICOFCS)* (pp. 66-74). Natal City, Brazil.

Deirmenjian, J. M. (1999), "Stalking in cyberspace," *Journal of the American Academy of Psychiatry and the Law Online* 27(3), pp. 407-413.

DeMarco, R. T. (2004). *Child pornography on the Internet-What to do?* Retrieved September 8, 2018, from http://www.crime-research.org/news/24.06.2004/446/

Dombrowski, S. C., LeMasney, J. W., Ahia, C. E., & Dickson, S. A. (2004), "Protecting children from online sexual predators: Technological, psychoeducational, and legal considerations," *Professional Psychology: Research and Practice* 35(1), pp. 65-73.

Dressing, H., Anders, A., Gallas, C., & Bailer, J. (2011), "Cyberstalking: Prevalence and impact on victims," *Psychiatrische Praxis* 38(7), pp. 336-341.

Ehrlich, I. (1973), "Participation in illegitimate activities: A theoretical and empirical investigation," *The Journal of Political Economy* 81(3), pp. 521-565.

Ellison, N. (2007), "Social network sites: Definition, history, and scholarship," *Journal of Computer-Mediated Communication* 13(1), pp. 210-230.

Erdur-Baker, Ö. (2010), "Cyberbullying and its correlation to traditional bullying, gender and frequent and risky usage of internet-mediated communication tools," *New Media & Society* 12(1), pp. 109-125.

Fairbanks, P. (2012). *Michigan man accused of cyberstalking 10 local females* Retrieved September 19, 2018, from http://quitstalkingme.com/2013/08/06/another-cyberstalking-case-involving-facebook-and-a-very-angry-person/

Federal Internet Law & Policy. (2012). *Cyberstalking*. Retrieved September 8, 2018, from http://www.cybertelecom.org/security/stalking.htm

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), pp. 257-308.

Fowler, G. A. (2012). *When the most personal secrets get outed on Facebook* Retrieved September 8, 2018, from http://online.wsj.com/article/SB10000872396390444165804578008740578200224.html

Fox, K. A., Gover, A. R., & Kaukinen, C. (2009), "The effects of low self-control and childhood maltreatment on stalking victimization among men and women," *American Journal of Criminal Justice* 34(3-4), pp. 181-197.

Fox, K. A., Nobles, M. R., & Akers, R. L. (2011), "Is stalking a learned phenomenon? An empirical test of social learning theory," *Journal of Criminal Justice* 39(1), pp. 39-47.

Fukuchi, A. (2011), "Balance of Convenience: The Use of Burden-Shifting Devices in Criminal Cyberharassment Law," *Boston College Law Review* 52(1), pp. 289-338.

Gauthier, D. K. (2001), "Professional lapses: Occupational deviance and neutralization techniques in veterinary medical practice," *Deviant Behavior* 22(6), pp. 467-490.

Goodno, N. H. (2007), "Cyberstalking, a new crime: Evaluating the effectiveness of current state and federal laws," *Missouri Law Review* 72(125), pp. 1-62.

Gottfredson, M. R. & Hirschi, T. (1990). *A General Theory of Crime*. Stanford, CA: Stanford University Press.

Grant, R. (2013). *How James Lasdun was haunted by a cyberstalker*. Retrieved September 19, 2018, from http://www.telegraph.co.uk/culture/books/authorinterviews/9854693/How-James-Lasdun-was-haunted-by-a-cyberstalker.html

Gregory, T. & Brekashvili, P. (2012). "Neutralization and whistleblowing: An empirical examination," Retrieved June 28, 2018, from http://aisel.aisnet.org/amcis2012/proceedings/PerspectivesIS/16/

Grodzinsky, F. S. & Tavani, H. T. (2002), "Some ethical reflections on cyberstalking," *ACM SIGCAS Computers and Society* 32(1), pp. 22-32.

Gross, R. & Acquisti, A. (2005, November 7), "*Information revelation and privacy in online social networks,"* Proceedings of the 2005 ACM Workshop on Privacy in the Electronic Society, Alexandria, VA, pp. 71-80.

Gutierrez, J. (2013). *Social media enables a new age of stalking*. Retrieved July 29, 2018, from http://www.dailytitan.com/2013/04/social-media-enables-a-new-age-of-stalking/

Hancock, B. (2000), "Cyberstalking on the Rise," *Computers & Security* 19(4), pp. 307-308.

Harrington, S. J. (1996), "The effect of codes of ethics and personal denial of responsibility on computer abuse judgments and intentions," *MIS Quarterly* 20(3), pp. 257-278.

Health 24. (2010). *Online sexual advances common for kids*. Retrieved September 8, 2018, from http://www.health24.com/Sex/Need-to-know/Online-sexual-advances-common-for-kids-20120721

Henry, S. (1990). *Degrees of Deviance: Student Accounts of Their Deviant Behavior*. Salem, WI: Sheffield Publishing Company.

Higgins, G. E. (2006), "Gender differences in software piracy: The mediating roles of self-control theory and social learning theory," *Journal of Economic Crime Management* 4(1), pp. 1-30.

Higgins, G. E. & Makin, D. A. (2004), "Does social learning theory condition the effects of low self-control on college students' software piracy," *Journal of Economic Crime Management* 2(2), pp. 1-22.

Hinduja, S. & Patchin, J. W. (2008), "Cyberbullying: An exploratory analysis of factors related to offending and victimization," *Deviant behavior* 29(2), pp. 129-156.

Holt, T. J. & Bossler, A. M. (2008), "Examining the applicability of lifestyle-routine activities theory for cybercrime victimization," *Deviant Behavior* 30(1), pp. 1-25.

Holtfreter, K., Reisig, M. D., & Pratt, T. C. (2008), "Low self-control, routine activities, and fraud victimization," *Criminology* 46(1), pp. 189-220.

Howes, O. D. (2006), "Compulsions in depression: stalking by text message," *The American Journal of Psychiatry* 163(9), pp. 1642-1642.

Hu, Q., Xu, Z., Dinev, T., & Ling, H. (2011), "Does deterrence work in reducing information security policy abuse by employees?," *Communications of the ACM* 54(6), pp. 54-60.

Huang, Y.-y. & Chou, C. (2010), "An analysis of multiple factors of cyberbullying among junior high school students in Taiwan," *Computers in Human Behavior* 26(6), pp. 1581-1590.

Hub Pages. (2013). *How to stalk people on Facebook using the close friends feature*. Retrieved September 19, 2018, from http://hubpages.com/hub/How-to-Stalk-People-on-Facebook-Using-the-Close-Friends-Feature

Huff Post Education. (2011). *Cyber-bullying: Are Boys Worse Than Girls?* Retrieved September 10, 2018, from http://www.huffingtonpost.com/2011/07/01/boys-worst-bullies-online_n_888529.html

Huff Post Politics. (2011). *Willow Palin Facebook posts: Homophobic slurs, curse words & more*. Retrieved September 14, 2018, from http://www.huffingtonpost.com/2010/11/16/willow-palin-facebook-posts_n_784585.html

Huff Post Tech. (2011). *Facebook cyberstalking shocker: preteen girls Charged In Issaquah Case* Retrieved September 19, 2018, from http://www.huffingtonpost.com/2011/04/27/facebook-cyberstalking-preteen-girls-charged_n_854605.html

Huffington Post & Salazar, C. (2011). *Alexis Pilkington Facebook horror: Cyber bullies harass teen even after suicide*. Retrieved September 8, 2018, from http://www.huffingtonpost.com/2010/03/24/alexis-pilkington-faceboo_n_512482.html

Jarvis, C. B., MacKenzie, S. B., & Podsakoff, P. M. (2003), "A critical review of construct indicators and measurement model misspecification in marketing and consumer research," *Journal of Consumer Research* 30(2), pp. 199-218.

Kamphuis, J. H. & Emmelkamp, P. M. (2000), "Stalking—A contemporary challenge for forensic and clinical psychiatry," *The British Journal of Psychiatry* 176(3), pp. 206-209.

Keith, M., Thompson, S. C., Hale, J., Lowry, P. B., & Greer, C. (2013), "Information disclosure on mobile devices: Proposing and testing an improved research methodology for capturing behaviour," *International Journal of Human-Computer Studies* forthcoming.

Khalifa, M. & Liu, V. (2007), "Online consumer retention: Contingent effects of online shopping habit and online shopping experience," *European Journal of Information Systems* 16(6), pp. 780-792.

Klockars, C. B. (1974). *The Professional Fence*. New York, NY: Free Press.

Koenigs, M., Kruepke, M., Zeier, J., & Newman, J. P. (2011), "Utilitarian moral judgment in psychopathy," *Social Cognitive and Affective Neuroscience* 7(6), pp. 708-714.

Kowalski, R. M., Limber, S. P., & Agatston, P. W. (2012). *Cyberbullying: Bullying in the digital age*. Malden, MA:Wiley-Blackwell.

Lamb, R. E. (1983), "Guilt, shame, and morality," *Philosophy and Phenomenological Research* 43(3), pp. 329 -346. Langer, G. (2013). *Attitudes shift against Snowden: Fewer than half say NSA is unjustified*. Retrieved July 29, 2018, from http://abcnews.go.com/blogs/politics/2013/07/attitudes-shift-against-snowden-fewer-than-half-say-nsa-is-unjustified/

Lee, J. & Lee, Y. (2002), "A holistic model of computer abuse within organizations," *Information Management & Computer Security* 10(2), pp. 57-63.

Lee, Y. (2011), "Understanding anti-plagiarism software adoption: An extended protection motivation theory perspective," *Decision Support Systems* 50(2), pp. 361-369.

Lenhart, A. (2009). *Cyberbullying and online teens* Retrieved September 8, 2018, from http://www.education.com/reference/article/cyberbullying-facts/

Li, W. & Cheng, L. (2013). Effects of neutralization techniques and rational choice theory on Internet abuse in the workplace, *Pacific Conference on Information Systems*. Jeju Island, Korea.

Limayem, M., Hirt, S. G., & Cheung, C. M. K. (2007), "How habit limits the predictive power of intention: The case of information systems continuance," *MIS Quarterly* 31(4), pp. 705-737.

Liston, B. (2013). "Cyberbullying investigated in suicide of Florida girl," Retrieved September 16, 2018, from http://www.reuters.com/article/2013/09/13/usa-florida-cyberbullying-idUSL2N0H91W520130913

Lowry, P. B., Curtis, A., & Lowry, M. R. (2004), "Building a taxonomy and nomenclature of collaborative writing to improve research and practice," *Journal of Business Communication* 41(1), pp. 66-99.

Lyndon, A., Bonds-Raacke, J., & Cratty, A. D. (2011), "College students' Facebook stalking of ex-partners," *Cyberpsychology, Behavior, and Social Networking* 14(12), pp. 711-716.

MacDonald, G. (2010). *Cyber-bullying defies traditional stereotype*. Retrieved September 8, 2018, from http://ww2.fairfaxtimes.com/cms/story.php?id=2078

Mail Online. (2007). *Girl, 13, commits suicide after being cyber-bullied by neighbour posing as teenage boy*. Retrieved September 19, 2018, from http://www.dailymail.co.uk/news/article-494809/Girl-13-commits-suicide-cyber-bullied-neighbour-posing-teenage-boy.html

Main, E. (2010). *Ronald McDonald is stalking your kids*. Retrieved July 29, 2018, from http://www.rodale.com/fast-food-advertising.

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

McCarthy, B. (2002), "New economics of sociological criminology," *Annual review of sociology* 28(pp. 417-442. McFarland, M. (2013). *How to get revenge*. Retrieved September 9, 2018, from http://www.howtodothings.com/family-relationships/100-ways-to-get-revenge

McFarlane, J. M., Campbell, J. C., Wilt, S., Sachs, C. J., Ulrich, Y., & Xu, X. (1999), "Stalking and intimate partner femicide," *Homicide Studies* 3(4), pp. 300-316.

McFarlane, L. & Bocij, P. (2003), "An exploration of predatory behaviour in cyberspace: Towards a typology of cyberstalkers," *First Monday* 8(9).

McVeigh, K. (2011). *Cyberstalking 'now more common' than face-to-face stalking*. Retrieved July 29, 2018, from http://www.guardian.co.uk/uk/2011/apr/08/cyberstalking-study-victims-men

Melnicoe, M. (2013). "California crackdown on 'Revenge Porn' in Brown's hands," Retrieved September 16, 2018, from http://www.bloomberg.com/news/2013-09-11/california-crackdown-on-revenge-porn-in-brown-s-hands.html

Meloy, J. R. (2001). *The Psychology of Stalking: Clinical and Forensic Perspectives*. San Diego, CA: Academic Press.

Meloy, J. R. & Gothard, S. (1995), "Demographic and clinical comparison of obsessional followers and offenders with mental disorders," *The American Journal of Psychiatry* 152(2), pp. 258-263.

Menesini, E., Nocentini, A., Palladino, B. E., Frisén, A., Berne, S., Ortega-Ruiz, R., et al. (2012), "Cyberbullying definition among adolescents: A comparison across six European countries," *Cyberpsychology, Behavior, and Social Networking* 15(9), pp. 455-463.

Mikhaylova, L. (2012). "Girls around me as a mirror of social networking," *Examiner.com*Retrieved September 20, 2018, from http://www.examiner.com/article/girls-around-me-as-a-mirror-of-social-networking

Miller, M. E. (2013). "Miami student Holly Jacobs fights revenge porn," Retrieved September 16, 2018, from http://www.miaminewtimes.com/2013-05-09/news/revenge-porn-miami-holly-jacobs/full/

Minor, W. W. (1981), "Techniques of neutralization: A reconceptualization and empirical examination," *Journal of Research in Crime and Delinquency* 18(2), pp. 295-318.

Mitchell, K. J., Finkelhor, D., & Wolak, J. (2007), "Youth internet users at risk for the most serious online sexual solicitations," *American Journal of Preventive Medicine* 32(6), pp. 532-537.

Muise, A., Christofides, E., & Desmarais, S. (2009), "More information than you ever wanted: Does Facebook bring out the green-eyed monster of jealousy?," *CyberPsychology & Behavior* 12(4), pp. 441-444.

Myyry, L., Siponen, M., Pahnila, S., Vartiainen, T., & Vance, A. (2009), "What levels of moral reasoning and values explain adherence to information security rules? An empirical study," *European Journal of Information Systems* 18(2), pp. 126-139.

Nagin, D. S. & Pogarsky, G. (2001), "Integrating celerity, impulsivity, and extralegal sanction threats into a model of general deterrence and evidence," *Criminology* 39(4), pp. 865-891.

Nansel, T. R., Overpeck, M., Pilla, R. S., Ruan, W., Simons-Morton, B., & Scheidt, P. (2001), "Bullying behaviors among us youth: Prevalence and association with psychosocial adjustment," *JAMA* 285(16), pp. 2094-2100.

National Crime Prevention Council. (2013). *Cyberbullying*. Retrieved September 8, 2018, from http://www.ncpc.org/cyberbullying

Neil Katz, A. H. (2010). *Samantha Kelly, 14, cyberbullied even after suicide*. Retrieved September 8, 2018, from http://www.cbsnews.com/8301-504763_162-20022676-10391704.html

Network for Surviving Stalking. (2013). *Stalker types*. Retrieved September 7, 2018, from http://www.nss.org.uk/about/stalking-facts-figures/stalker-types/

O'Keeffe, G. S., Clarke-Pearson, K., Communications, C. o., & Media. (2011), "The impact of social media on children, adolescents, and families," *Pediatrics* 127(4), pp. 800-804.

Olthof, T., Ferguson, T., Bloemers, E., & Deij, M. (2004), "Morality- and identity- related antecedents of children's guilt and shame attributions in events involving physical illness," *Cognition & Emotion* 18(3), pp. 383-404.

Oremus, W. (2013). *Study: Twitter is full of haters*. Retrieved September 8, 2018, from http://www.slate.com/blogs/future_tense/2013/03/04/pew_internet_survey_twitter_is_full_of_haters_and_negative_opinions.html.

Palarea, R. E., Zona, M. A., Lane, J. C., & Langhinrichsen-Rohling, J. (1999), "The dangerous nature of intimate relationship stalking: Threats, violence, and associated risk factors," *Behavioral Sciences & the Law* 17(3), pp. 269-283.

Parker, D. B. (1983). *Fighting Computer Crime*. New York: Scribner New York.

Patchin, J. W. & Hinduja, S. (2010), "Cyberbullying and self-esteem," *Journal of School Health* 80(12), pp. 614-621.

Petherick, W. (2001). *Cyberstalking: Obsessional pursuit and the digital criminal*. Retrieved September 8, 2018, from http://www.crimelibrary.com/criminology/cyberstalking/index.html.

Petherick, W. (2003). *Cyber-stalking: obsessional pursuit and the digital criminal*. Retrieved September 19, 2018, from http://www.trutv.com/library/crime/criminal_mind/psychology/cyberstalking/5.html

Pettinari, D. (2013). *Cyberstalking investigation and prevention*. Retrieved September 8, 2018, from http://www.crime-research.org/library/Cyberstalking.htm.

Philips, F. & Morrissey, G. (2004), "Cyberstalking and cyberpredators: A threat to safe sexuality on the Internet," *Convergence: The International Journal of Research into New Media Technologies* 10(1), pp. 66-79.

Picard, P. (2007). *Teen research unlimited, tech abuse in teen relationships study*. Retrieved September 9, 2018, from http://www.loveisnotabuse.com/c/document_library/get

Piquero, A. & Tibbetts, S. (1996), "Specifying the direct and indirect effects of low self-control and situational factors in offenders' decision making: Toward a more complete model of rational offending," *Justice Quarterly* 13(3), pp. 481-510.

Pittaro, M. L. (2007), "Cyber stalking: An analysis of online harassment and intimidation," *International Journal of Cyber Criminology* 1(2), pp. 180-197.

Polites, G. L. & Karahanna, E. (2013), "The embeddedness of information systems habits in organizational and individual level routines: Development and disruption," *MIS Quarterly* 37(1), pp. 221-246.

Posey, C., Roberts, T. L., Lowry, P. B., Bennett, R. J., & Courtney, J. (2013), "Insiders' protection of organizational information assets: Development of a systematics-based taxonomy and theory of diversity for protection-motivated behaviors," *MIS Quarterly* 37(4), pp. 1189-1210.

Potter, T. (2012). *Why be a victim of a cyber stalker*. Retrieved September 14, 2018, from http://www.timpotter-philippines.com/2012/12/tim-potter-from-sugar-land-texas-being.html

Press Association. (2013). *Scottish teenager 'killed himself over online blackmail threats'*. Retrieved September 8, 2018, from http://www.theguardian.com/uk-news/2013/aug/16/scottish-teenager-online-blackmail-skype

Prismacat. (2010). *Samantha Kelly bullied to death: Mich. 14-year-old's suicide followed harassment after rape claim*. Retrieved September 9, 2018, from http://www.cbsnews.com/8618-504083_162-20022556.html?assetTypeId=41&messageId=10063173

Puhakainen, P. & Ahonen, R. (2006). *Design theory for information security awareness.* University of Oulu, Oulu, Finland.

QuitStalkingMe. (2011). *Ten reasons why someone is stalking you online*. Retrieved September 7, 2018, from http://quitstalkingme.com/2011/07/28/ten-reasons-why-someone-is-stalking-you-online/

QuitStalkingMe. (2013). *Another cyberstalking case involving Facebook and a very angry person*. Retrieved September 19, 2018, from http://quitstalkingme.com/2013/08/06/another-cyberstalking-case-involving-facebook-and-a-very-angry-person/

Read Daily News. (2013). *Li Yuchun "death" accused denied the poster*. Retrieved September 14, 2018, from http://www.readdailynews.com/news-4331028-Li-Yuchun-death-accused-denied-the-poster.html

Reyns, B. W., Henson, B., & Fisher, B. S. (2011), "Being pursued online applying cyberlifestyle–Routine activities theory to cyberstalking victimization," *Criminal Justice and Behavior* 38(11), pp. 1149-1169.

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), pp. 1-25.

Ripabrelli, L. (2011). *12-year-old sentenced for cyberstalking classmate*. Retrieved September 19, 2018, from http://abcnews.go.com/Technology/12-year-sentenced-washington-cyberstalking-case/story?id=14072315

Rivera, Z. (2013). *Daddy Yankee's rep dismisses gay rumors after online photo sparks speculation*. Retrieved September 14, 2018, from http://www.nydailynews.com/entertainment/gossip/daddy-yankee-gay-rep-article-1.1307589

Rogers, M. K. (2001). *A Social Learning Theory and Moral Disengagement Analysis of Criminal Computer Behavior:An Exploratory Study*. University of Manitoba.

Rouse, M. (2010). *Cyberbullying*. Retrieved September 9, 2018, from http://whatis.techtarget.com/definition/cyberbullying

Salazar, C. (2010). *Alexis Pilkington Facebook horror: Cyber bullies harass teen even after Suicide*. Retrieved September 9, 2018, from http://www.huffingtonpost.com/2010/03/24/alexis-pilkington-faceboo_n_512482.html

Salmivalli, C., Lagerspetz, K., Björkqvist, K., Österman, K., & Kaukiainen, A. (1996), "Bullying as a group process: Participant roles and their relations to social status within the group," *Aggressive Behavior* 22(1), pp. 1-15.

SAPAC. (2013). *Types of stalkers*. Retrieved September 7, 2018, from http://sapac.umich.edu/article/320

Schreck, C. J. (1999), "Criminal victimization and low self-control: An extension and test of a general theory of crime," *Justice Quarterly* 16(3), pp. 633-654.

Schreck, C. J., Stewart, E. A., & Osgood, D. W. (2008), "A reappraisal of the overlap of violent offenders and victims," *Criminology* 46(4), pp. 871-906.

Seipel, C. & Eifler, S. (2010), "Opportunities, rational choice, and self-control on the interaction of person and situation in a general theory of crime," *Crime & Delinquency* 56(2), pp. 167-197.

Sheridan, L. & Davies, G. M. (2001), "Stalking: The elusive crime," *Legal and Criminological Psychology* 6(2), pp. 133-147.

Shouse Law Group. (2013). *California cyberstalking stalking laws*. Retrieved September 8, 2018, from http://www.shouselaw.com/cyberstalking.html

Siponen, M. & Vance, A. (2010), "Neutralization: New insights into the problem of employee information systems security policy violations," *MIS Quarterly* 34(3), pp. 487-502.

Siponen, M., Vance, A., & Willison, R. (2012), "New insights into the problem of software piracy: The effects of neutralization, shame, and moral beliefs," *Information & Management* 49(7–8), pp. 334-341.

Skinner, W. F. & Fream, A. M. (1997), "A social learning theory analysis of computer crime among college students," *Journal of Research in Crime and Delinquency* 34(4), pp. 495-518.

Sleglova, V. & Cerna, A. (2011). "Cyberbullying in adolescent victims: Perception and coping," *Cyberpsychology:Journal of Psychosocial Research on Cyberspace* 5(2), Retrieved, from http://cyberpsychology.eu/view.php?cisloclanku=2011121901&article=4

Smith, P. K., Mahdavi, J., Carvalho, M., Fisher, S., Russell, S., & Tippett, N. (2008), "Cyberbullying: Its nature and impact in secondary school pupils," *Journal of Child Psychology and Psychiatry* 49(4), pp. 376-385.

Solutions Blog. (2010). *Cyber-bullying and social networking identity theft*. Retrieved September 19, 2018, from http://www.sileo.com/cyber-bullying-and-social-networking-identity-theft/

Sourander, A., Brunstein Klomek, A., Ikonen, M., Lindroos, J., Luntamo, T., Koskelainen, M., et al. (2010), "Psychosocial risk factors associated with cyberbullying among adolescents: A population-based study," *Archives of General Psychiatry* 67(7), pp. 720-728.

Spitzberg, B. (2000, November 3-6), "*Forlorn love: Attachment styles, love styles, loneliness, and obsessional thinking as predictors of obsessive relational intrusion,"* National Communication Association Conference, Seattle, WA.

Spitzberg, B. H. & Cupach, W. R. (2001), "Paradoxes of pursuit: Toward a relational model of stalking-related phenomena," In J. Davis (Ed.), *Stalking Crimes and Victim Protection: Prevention, Intervention, Threat Assessment, and Case Management* (pp. 97-136). Boca Raton, FL: CRC Press.

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

Spitzberg, B. H. & Rhea, J. (1999), "Obsessive relational intrusion and sexual coercion victimization," *Journal of Interpersonal Violence* 14(1), pp. 3-20.

Star-Telegram. (2013). *Loving, denigrating, profane text messages read during counselor trial*. Retrieved September 8, 2018, from http://www.star-telegram.com/2013/02/13/4619426/loving-denigrating-profane-text.html

Stocker, M. & Nielssen, O. (2000). Apprehended violence orders and stalking, *Stalking: Criminal Justice Response Conference*. Sydney.

Sykes, G. M. & Matza, D. (1957), "Techniques of neutralization: A theory of delinquency," *American Sociological Review* 22(6), pp. 664-670.

Tangney, J. P., Miller, R. S., Flicker, L., & Barlow, D. H. (1996), "Are shame, guilt, and embarrassment distinct emotions?," *Journal of Personality and Social Psychology* 70(6), pp. 1256-1269.

Tavani, H. T. (2000), "Defining the boundaries of computer crime: Piracy, break-ins, and sabotage in cyberspace," *ACM SIGCAS Computers and Society* 30(3), pp. 3-9.

Tavani, H. T. (2002), "The uniqueness debate in computer ethics: What exactly is at issue, and why does it matter?," *Ethics and Information Technology* 4(1), pp. 37-54.

Tavani, H. T. & Grodzinsky, F. S. (2002), "Cyberstalking, personal privacy, and moral responsibility," *Ethics and Information Technology* 4(2), pp. 123-132.

Telegraph Reporters. (2013). *'True stalker' former footballer drove ex-girlfriend to brink of suicide*. Retrieved July 29, 2018, from http://www.telegraph.co.uk/news/uknews/crime/10054161/True-stalker-former-footballer-drove-ex-girlfriend-to-brink-of-suicide.html

The Times of India. (2013). *Student in dock for profane FB attack on friend*. Retrieved September 14, 2018, from http://articles.timesofindia.indiatimes.com/2013-05-09/hyderabad/39141964_1_fake-facebook-ravi-abusive-messages

Tibbetts, S. G. & Gibson, C. L. (2002), "Individual propensities and rational decision-making: Recent findings and promising approaches," In A. R. Piquero & S. G. Tibbetts (Eds.), *Rational Choice and Criminal Behavior Recent Research and Future Challenges* (pp. 3-24). New York, NY: Routledge.

Tjaden, P. G. & Thoennes, N. (1998). *Stalking in America: Findings from the National Violence Against Women Survey*.

Washington, DC: US Department of Justice, Office of Justice Programs, National Institute of Justice.

Tjaden, P. G. & Thoennes, N. (2000). *Extent, Nature, and Consequences of Intimate Partner Violence*. Washington, DC: US Department of Justice, Office of Justice Programs, National Institute of Justice

Tokunaga, R. S. (2010), "Following you home from school: A critical review and synthesis of research on cyberbullying victimization," *Computers in Human Behavior* 26(3), pp. 277-287.

University, N. (2013). *Fake Facebook friends*. Retrieved September 20, 2018, from http://www.northeastern.edu/securenu/?page_id=471

US Attorney General. (1999). "Cyberstalking: A new challenge for law enforcement and industry: A report to congress," Retrieved September 20, 2018, from http:/www.usdoj.gov/ag/cyberstalkingreport.htm

US Legal. (2013). *Cyber bullying law & legal definition*. Retrieved September 8, 2018, from http://definitions.uslegal.com/c/cyber-bullying/

Vance, A. & Siponen, M. (2012), "IS security policy violations: A rational choice perspective," *Journal of Organizational and End-User Computing* 24(1), pp. 21-41.

Vandebosch, H. & Van Cleemput, K. (2009), "Cyberbullying among youngsters: Profiles of bullies and victims," *New Media & Society* 11(8), pp. 1349-1371.

von Marées, N. & Petermann, F. (2012), "Cyberbullying: An increasing challenge for schools," *School Psychology International* 33(5), pp. 467-476.

Wealth Creation. (2013, June 26, 2013). *Mobile spy: Monitor the activity of your boy/girl friend In real time*. Retrieved September 14, 2018, from http://www.yomiprof.com/2013/06/mobile-spy-monitor-activity-of-your.html.

Weaver, R. (2010). *Gang stalking: Psychological targeting in a group setting*. Retrieved September 8, 2018, from http://www.empowher.com/mental-health/content/gang-stalking-psychological-targeting-group-setting.

Weir, G. R., Toolan, F., & Smeed, D. (2011), "The threats of social networking: Old wine in new bottles?," *Information Security Technical Report* 16(2), pp. 38-43.

Wellbelove, C. (2008). *Fake profiles on Facebook, is someone pretending to be you?* Retrieved September 9, 2018, from http://wellbelove.com/2008/06/16/fakefacebookprofiles/

Westrup, D. & Fremouw, W. J. (1998), "Stalking behavior: A literature review and suggested functional analytic assessment technology," *Aggression and Violent Behavior* 3(3), pp. 255-274.

Wikipedia. (2013a). *Cyberstalking*. Retrieved September 7, 2018, from http://en.wikipedia.org/wiki/Cyberstalking

Wikipedia. (2013b). *Edison Chen*. Retrieved Sept 19, 2018, from http://en.wikipedia.org/wiki/Edison_Chen#2008_photo_scandal.

Wikipedia. (2013c). *Manti Te'o*. Retrieved September 9, 2018, from http://en.wikipedia.org/wiki/Manti_Te'o

WiredSafety. (2013). *What is cyberbullying, exactly?* Retrieved September 8th, 2018, from http://stopcyberbullying.org/what_is_cyberbullying_exactly.html

Ybarra, M. L. (2004), "Linkages between depressive symptomatology and Internet harassment among young regular Internet users," *CyberPsychology & Behavior* 7(2), pp. 247-257.

Ybarra, M. L., Mitchell, K. J., Wolak, J., & Finkelhor, D. (2006), "Examining characteristics and associated distress related to Internet harassment: Findings from the Second Youth Internet Safety Survey," *Pediatrics* 118(4), pp. e1169-e1177.

Young, L., Koenigs, M., Kruepke, M., & Newman, J. P. (2012), "Psychopathy increases perceived moral permissibility of accidents," *Journal of Abnormal Psychology* 121(3), pp. 659-667.

Yourself Series. (2013). *Bonus YSS: Are you a cyber-bully?* Retrieved September 8, 2018, from http://yourselfseries.com/teens/topic/cyberbullying/bonus-yss-are-you-a-cyber-bully/

Zur, O., Williams, M. H., Lehavot, K., & Knapp, S. (2009), "Psychotherapist self-disclosure and transparency in the Internet age," *Professional Psychology: Research and Practice* 40(1), pp. 22-30.