

Friend or Foe: Cyberbullying in Social Network Sites

Sixuan Zhang
Baylor University

Liang Yu
HuaTai Securities Co.,Ltd.

Robin L. Wakefield
Baylor University

Dorothy E. Leidner
Baylor University,
The University of Lund

Acknowledgment

The authors thank the Hankamer School of Business at Baylor University for their generous support of this research as well as the editor and anonymous reviewers for their helpful guidance during the revision of this manuscript.

Abstract

As the use of social media technologies proliferates in organizations, it is important to understand the nefarious behaviors, such as cyberbullying, that may accompany such technology use and how to discourage these behaviors. We draw from neutralization theory and the criminological theory of general deterrence to develop and empirically test a research model to explain why cyberbullying may occur and how the behavior may be discouraged. We created a research model of three second-order formative constructs to examine their predictive influence on intentions to cyberbully. We used PLS-SEM to analyze the responses of 174 Facebook users in two different cyberbullying scenarios. Our model suggests that neutralization techniques enable cyberbullying behavior and while sanction certainty is an important deterrent, sanction severity appears ineffective. We discuss the theoretical and practical implications of our model and results.

Keywords: Cyberbullying, Social Network Sites, Neutralization theory, Deterrence theory, Facebook, Shame, Sanctions, Intentions

ACM Categories: H.1.1

General Terms: Human factors

Introduction

The popular media has denounced cyberbullying behavior on account of the tragic consequences that have resulted in several high-profile cases, such as the freshman suicide at Rutgers University due to a Twitter message that made a private moment public (Foderaro, 2010). Cyberbullying is defined as “an aggressive, intentional act carried out by a group or individual using electronic forms of contact repeatedly and over time against a victim who cannot easily defend him or herself” (Smith et al., 2008; p. 376). The main attributes of cyberbullying include aggression, intention, repetition and power imbalance (Dooley, Pyżalski & Cross, 2009; Kernaghan & Elwood, 2013). Cyberbullying is also described as a malicious act that may occur over various communication modes including phone, text messaging, e-mails, pictures/video clips, instant messaging, websites, and chat rooms (Smith et al., 2008). Cyberbullying is considered worse than traditional bullying due to the types of injury that may result such as higher depression rates and stronger negative feelings (Cassidy, Faucher & Jackson, 2013; Gorzig & Frumkin, 2013). Many acts of cyberbullying have been executed in social network sites (SNSs). The Pew Research Center states that 39 percent of SNS users are likely to experience some form of cyberbullying (Skye, 2012).

Moreover, picture or video clip bullying in SNSs is considered to have the largest negative impact (Smith et al., 2008).

The typical features of social media such as “friends,” “comments” and “photos” make SNSs suitable platforms for the display of aggressive and/or offensive behaviors toward another individual or user (Boyd & Ellison, 2007). Furthermore, since digital content posted on SNSs can be quickly and widely disseminated, a single act such as posting an insulting comment or a compromising picture may result in continued and repeated humiliation for the victim (Kernaghan & Elwood, 2013). The ability to connect to a large audience in a short period of time makes SNS cyberbullying a severe form of aggression compared to traditional bullying (Sticca & Perren, 2013). Additionally, because cyberbullying may be perpetrated anonymously and the victim may be unable to distance himself from the embarrassment, to delete the content, or to deny falsehoods in a SNS, the victim’s feelings of frustration, helplessness and powerlessness are likely to increase (Badiuk, 2006; Kernaghan & Elwood, 2013; Mishna, Saini & Solomon, 2009; Sticca & Perren, 2013,).

Research indicates that cyberbullying may begin as early as elementary school, reach the highest level during middle school years, and slightly decrease in high school (Rivituso, 2012). In fact, the prevalence of cyberbullying among college-aged students was found to range from 10 to 28.7 percent, and 25 percent of the time occurred via a SNS (Zalaquett & Chatters, 2014). While the issue of bullying, in general, and cyberbullying, in particular, is often regarded as a childhood problem, there is growing evidence that this behavior also occurs in the workplace (Dobson, 2012). General workplace bullying has been implicated in negative job-related effects such as absenteeism and lower levels of job satisfaction (Dooley et al., 2009; Kivimaki, Elovainio, & Vahtera, 2000; Quine, 1999) which should concern organizations if workplace bullying is moving online. Given that social media is becoming more common in organizations (Kiron et al., 2012) with the economic impact of organizational social media expected to surpass \$1 trillion (Chui, et al., 2012), it is prudent to examine the risks associated with this tool.

As yet, it is unclear how social media and SNSs will impact the organization and its employees. Therefore, managers face a challenge as they seek to implement novel ways of organizational communication and interaction using social media. The objective of our study is to identify and examine factors that may allow cyberbullying behavior to occur as well as factors that would inhibit the behavior. Specifically, we investigate the cyberbullying behaviors of young adults under the assumption that this group is likely to

bring similar patterns of behavior into the workplace. More specifically, our study addresses the following research questions: 1) Why does cyberbullying occur in SNSs among young adults? 2) What are effective deterrents to cyberbullying behavior in SNSs? We draw from neutralization theory and the criminological theory of general deterrence to develop and empirically test our research model. Facebook serves as the context for this study since Facebook is the most popular SNS with over 1.31 billion active users (Facebook Statistics, 2014), and 26 percent of all Facebook users are in the 18-25 age range (Kenburary, 2011). Our study is focused at the construct level in which higher-order formative factors are modeled to explore the antecedents of cyberbully behavior within a nomological network that includes justification and deterrence, rather than at the measurement item level. Thus, our study offers theoretical as well as practical implications.

Theoretical Background

Our research model is founded on two theories from the field of Criminology: neutralization theory (Sykes & Matza, 1957) and general deterrence theory (Paternoster & Simpson, 1996). Neutralization theory describes the reasoning behind why one might engage in deviant behavior, such as cyberbullying, and deterrence theory describes how deviant behavior may be prevented.

Neutralization Theory

Neutralization theory assumes that the norms of the community are agreed to by both law-abiding individuals and lawbreakers, but delinquency results from an unconscious defense of deviant behavior (Sykes & Matza, 1957). Thus, in an attempt to justify his own delinquent behavior, the law-breaker would view unacceptable behavior as valid. These justifications are known as neutralization techniques. Five neutralization techniques have been proposed including denial of responsibility, denial of injury, denial of the victim, condemnation of the condemners, and appeal to higher loyalties (Sykes & Matza, 1957) that the offender may assert to justify bad behavior.

We suggest that denial, rather than naiveté, is involved in cyberbullying because educational initiatives in public school systems often include presentations to warn students about inappropriate online behavior such as cyberbullying (Ahmed, Harris, & Braithwaite, 2006). Public media has also warned society as a whole of the negative consequences of cyberbullying (Dooley et al., 2009). Given the attention to cyberbullying in schools and the media, it is likely that young adults are aware of the potential for social media to be used as a cyberbullying tool. Consequently, the use of SNSs to cyberbully is

unlikely to be inadvertent, but rather an intentional act. Since cyberbullying is not a face-to-face behavior, perpetrators can avoid seeing the victims' pain and emotional distress (Cassidy, Faucher & Jackson, 2013). Invisibility to the outcome may facilitate cyberbully behavior if the lack of a face-to-face encounter enables the perpetrator to deny that harm was done. Additionally, cyberbullies may treat the asynchronous communication of SNSs as an escape route if they feel they can distance themselves from the harmful communicate. For example, asynchrony may contribute to denial if it enables the cyberbully to avoid responsibility, "It feels safe putting the message out there where it can be left behind" (Suler, 2004, pp. 323). Thus, in accordance with neutralization theory, a cyberbully is likely to understand what constitutes cyberbullying behavior but may defend his/her actions based on denials that arise from the ability to distance himself from the encounter via the characteristics of SNSs, such as asynchronicity.

We propose that the cyberbully justifies offensive online behavior through several of the processes of denial described in neutralization theory. Our research model examines and tests three neutralization constructs most related to cyberbullying in SNS: denial of responsibility, denial of injury and denial of the victim. Two neutralization techniques, condemnation of the condemners and appeal to higher loyalties, are omitted from the model for several reasons. First, condemnation of the condemners means the delinquent attributes his own anti-social behaviors to those disapproving these violations. In the context of SNS, this would mean the cyberbully might justify his behavior by drawing attention to the anti-cyberbullying policies of the SNS and focusing on their unreasonableness. The appeal to higher loyalties construct describes how social norms may be neutralized by sacrificing the needs of the larger community for the needs of the smaller social group in which the delinquent participates. In this case, it might be that cyberbullying is in the best interest of the delinquent's online social 'community.' Based on prior research, there is little support for these two constructs as neutralizing rationales for cyberbullying. Additionally, studies based on neutralization theory often use the most applicable subset of the neutralization techniques (Cao, 2004; Siponen & Vance, 2010). Thus, our study includes the three dimensions most related to cyberbullying in SNSs that are discussed below.

Denial of Responsibility

According to the denial of responsibility neutralization technique, the delinquent shifts accountability for a deviant behavior to another party by claiming that the environment or outside factors are responsible for his behavior (Sykes & Matza, 1957). For example, in an effort to absolve himself of responsibility, the delinquent may attribute his harmful behaviors to environmental factors such as bad companions or a poor childhood. Interestingly, research indicates that perpetrators and bystanders are more likely to attribute the responsibility for cyberbullying to the victim when the victim appears to be extroverted and willingly discloses personal information online (Weber, Ziegele & Schnauber, 2013). Morrison (2006) found that when a perpetrator took responsibility for his cyberbullying acts, his social ties strengthened and he was more likely to perform good deeds in the future. In contrast, when individuals shifted the responsibility for their cyberbullying, they were more likely to continue to cyberbully. We surmise that a SNS cyberbully who shifts the responsibility for his actions by blaming others or environmental circumstances is using the denial of responsibility technique to rationalize his offenses. This neutralization technique relieves the perpetrator of personal culpability and may allow offensive behavior to continue or escalate.

Denial of Injury

The denial of injury construct describes a delinquent who believes that his offensive behavior is not harmful even though social norms dictate otherwise (Sykes & Matza, 1957). Thus, the perpetrator may acknowledge the offensiveness of cyberbullying but may rationalize that 'it's not a big deal' or 'it didn't do much harm.' Just as the delinquent uses denial of responsibility to distance himself from his behavior, he may also use denial of injury to break the link between his behavior and the consequences. Research shows that almost 40 percent of those who cyberbullied others also reported engaging in online harassment for fun (Raskauskas & Stoltz, 2007). Clearly there is a denial of the potential for harm. Research suggests that a denial or diminishment of the consequences of an action also reduces the likelihood of empathy for the victim and remorse for the behavior (Dooley et al., 2009). In addition, because of the absence of social presence in online environments, cyberbullies may underestimate the harmfulness of their actions in SNSs. If one believes that an act of cyberbullying is not injurious or the outcome is inconsequential, then there is little motivation to discontinue or shun the behavior.

Denial of Victim

The denial of victim technique claims that any injury caused by delinquent behavior is nothing more than a justified retaliation. In effect, the delinquent positions himself as an innocent victim and transforms the victim into the wrong-doer (Sykes & Matza, 1957). In this situation the cyberbully would view himself as 'in the right' and his aggressive action as justifiable because the other party 'had it coming.' In a study of adolescent bullying behavior, 25 percent of those who admitted to cyberbullying claimed they committed the behavior to 'get back at someone they're mad at' (Raskauskas & Stoltz, 2007). Marcum *et al.* (2013) reported that both males and females were more likely to cyberbully via Facebook if they had been bullied previously. Thus, a prior victimization may facilitate cyberbullying behavior for retaliatory purposes. Using the denial of victim technique, the victim is denied his 'victim-hood' because the cyberbully believes that he or she is simply righting a wrong.

Deterrence Theory

Deterrence theory involves the nature and effect of sanctions against those who commit a deviant act. Sanctions are represented by two aspects that include 1) the certainty of sanctions, and 2) the severity of sanctions (Blumstein, Cohen, & Nagin, 1978). Individuals are less likely to commit antisocial acts if the risk of getting caught (certainty of sanctions) is high and the penalties for violation (severity of sanctions) are severe. Furthermore, deterrence theory has been extended to include informal sanctions and shame (Siponen & Vance, 2010). Informal sanctions refer to the disapproval and/or criticism of an action by families, peers or the community to which the individual belongs (Paternoster & Simpson, 1996). Shame is defined as a genuine feeling of guilt or disgrace if others know of one's deviant behavior (Eliason & Dodder, 1999). Researchers propose that shame should be separated from informal and formal sanctions because it is self-imposed (Paternoster & Simpson, 1996), although it may be regarded as a deterrent because it has effects similar to other sanctions (Eliason & Simpson, 1995).

Although most cyberbullying cases are not prosecutable crimes, they are often portrayed in the public as behavior that must be controlled or deterred. Thus, formal sanctions for behavior rising to the level of 'cyberbullying' are often described in SNS policies and user guidelines. For example, formal sanctions in Facebook may include disabling a user account or partially restricting a user's access to the SNS (Facebook, 2012). The disapproval of peers, family and the online community characterizes informal sanctions that may inhibit cyberbullying. Bastiaensens

(2014) suggests that peers and bystanders should discourage cyberbullies in SNSs and Cassidy *et al.* (2013) emphasizes the positive roles of parents and the community in restraining the cyberbullying problem. Shame has been an effective deterrent for traditional bullying and may likewise apply to cyberbullying if SNS users believe certain behaviors are shameful and immoral. In sum, we adopt formal sanctions, informal sanctions and shame from deterrence theory to construct our research model.

Research Model

The research model shown in Figure 1 depicts three multidimensional constructs: Neutralization, Certainty of Sanctions and Severity of Sanctions. Each multidimensional construct is a second-order molar factor. Neutralization is a formative second-order construct comprised of three dimensions: Denial of Responsibility, Denial of Injury and Denial of Victim. Certainty of Sanctions and Severity of Sanctions are also second-order formative constructs each comprised of three dimensions. The dependent variable in the model is intention to cyberbully. The intention to perform some behavior may be viewed as "an indicator of a motivational state that exists just prior to the commission of an act" or as "a measured reflection of a predisposition to commit an act" (Paternoster & Simpson 1996, p. 561). Additionally, intention is often operationalized in the literature as a proxy for behavior based on the work of Fishbein and Ajzen (1975).

Neutralization and Intention to Cyberbully

Neutralization is defined as the justifications used by delinquents to rationalize their deviant behavior (Sykes & Matza, 1957). It is a multi-dimensional construct comprised of three dimensions, Denial of Responsibility, Denial of injury and Denial of victim, that are considered distinct facets of neutralization (Jarvis, Mackenzie, & Podsakoff, 2003; Siponen & Vance, 2010). Each neutralization dimension describes a specific means by which an individual may nullify the risks to himself of cyberbullying in order to justify executing the behavior in a SNS.

The three dimensions are formative dimensions of neutralization and each is modeled reflectively because its associated measurement items are uni-dimensional, correlated, reflect the dimension, and are a representation of the dimension (Petter, Straub, & Rai, 2007; Gefen, Straub & Boudreau, 2000). Neutralization has been modeled in this manner in the Information Systems (IS) literature in order to focus on the neutralization strategies used to justify IS security violations (Siponen & Vance, 2010).

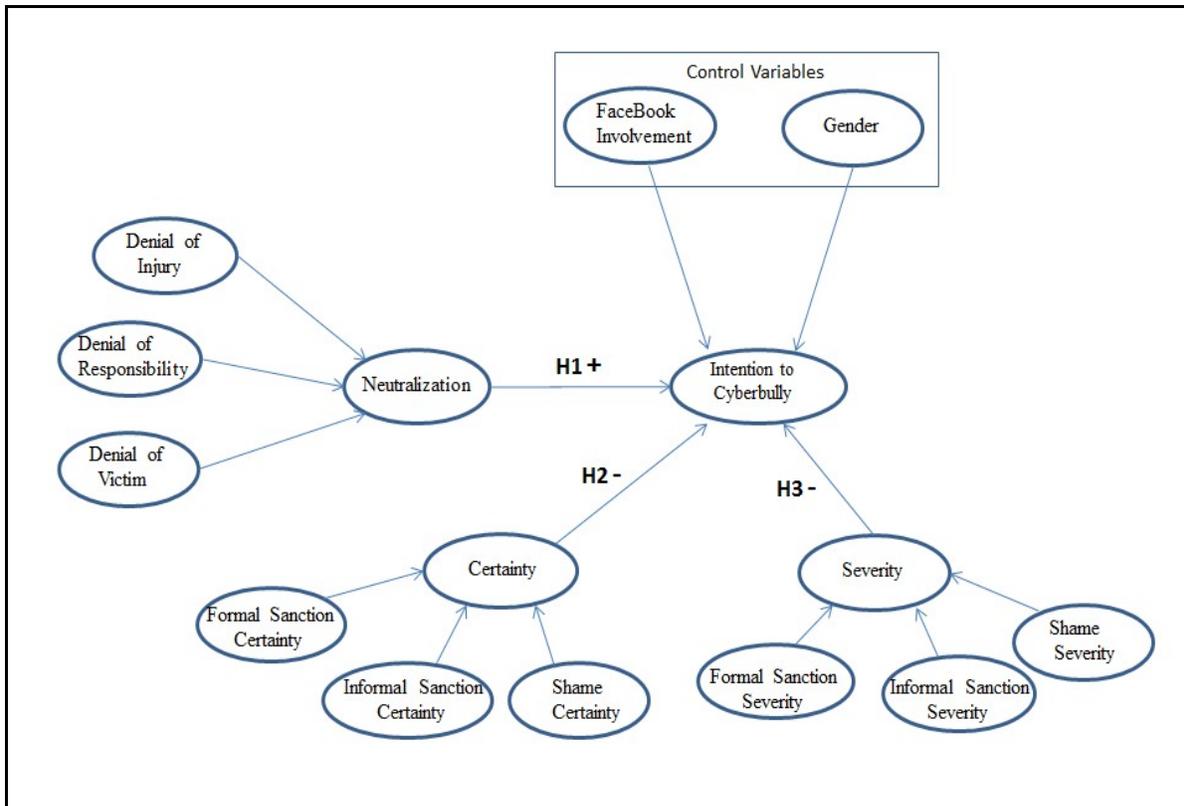


Figure 1. Research Model

The content validity of the formative construct is established with the inclusion of the major aspects of the construct's domain (denial of injury, responsibility and victim) that are applicable to cyberbullying (c.f., Diamantopoulos, 2011) and have been discussed previously. As a second-order construct neutralization is a complex factor and exploring the relative effects of each first-order dimension will clarify the processes through which cyberbullying arises.

Because neutralization encompasses the means to rationalize one's behavior (via the first-order dimensions), those who cyberbully in Facebook are likely to justify their intended behavior prior to performing the behavior. We expect that the cyberbully has absolved him/herself prior to the action in order to perform the action. Research found that employees that neutralized their behavior were more likely to violate IS security policies (Siponen & Vance, 2010), the justification precedes the action. Due to media publicity and public school efforts to eliminate cyberbullying, we assume that young adults are acutely aware of what constitutes this behavior. Thus, neutralizing the behavior would occur prior to the action and would then lead to the formation of intentions. Based on the above discussion of the multi-dimensional nature of neutralization, we hypothesize the following:

Hypothesis 1 (H1): Neutralization is positively associated with intentions to cyberbully in Facebook.

Certainty of Sanctions and Severity of Sanctions

Sanctions represent disincentives and in the context of cyberbullying the construct is comprised of formal sanctions, informal sanctions and shame. Formal sanctions are the implementation of stated consequences that would result from cyberbullying behavior. It is typical for SNSs to post policies stating objectionable behaviors as well as consequences for performing those behaviors. Posted policies and user guidelines are often conditions with which the user must 'agree' before activating the site. For example, in the "Statement of Rights and Responsibilities" of Facebook (2012), the consequences of cyberbullying in Facebook are described as "disable your account," "stop providing all of Facebook to you," and "stop providing part of Facebook to you." It is expected that these formal sanctions would activate cost/benefit considerations (Blumstein et al., 1978) in the decision to engage in cyberbullying and serve as a disincentive.

Informal sanctions are potential costs or risks that may not be explicitly stated or policy-driven, but nevertheless may result from the commission of a deviant act. Informal sanctions may include job loss, social and personal embarrassment or the disapproval

of friends or family (Paternoster & Simpson, 1996). In Facebook, every user is connected with 'friends' and many are also connected with family members and belong to Facebook communities. Thus, informal sanctions are related to the loss of respect from one's friends, family members and/or communities when they become aware of one's cyberbullying behavior. Deterrence Theory and rational choice support the argument that one will often choose to act in one's own self-interest when weighing benefits and risks. Because cyberbullying behavior may result in media attention when the consequences are tragic or may be shared within SNS communities, the risk of others knowing of one's behavior serves as an informal deterrent (Cassidy et al., 2013).

The third facet of sanctions is shame. Shame is depicted as an emotional state or condition characterized by embarrassment, dishonor, disgrace and humiliation (Broucek, 1991). While shame may be considered a type of informal sanction, it has been conceptually differentiated from informal sanctions because of its self-imposing nature (Paternoster & Simpson 1996). Whereas informal sanctions originate from what others think and may result in the loss of respect for a cyberbully, shame is self-inflicted and originates within the one who victimizes others. Thus, shame is a separate and independent dimension of sanctions. Traditionally, shame has been an effective deterrent of anti-social behaviors and thus is expected to operate as an important facet of sanctions. Shame may be managed by the individual in two ways: shame acknowledgment and shame displacement (Morrison, 2006). Shame acknowledgment is the acceptance of responsibility for a wrong committed while shame displacement blames others for the wrong and denies any responsibility of a harmful behavior (Ahmed, Harris, & Braithwaite, 2006). Shame management processes were found to be a significant variable in understanding general bullying behavior (Ahmed et al., 2001) in that shame acknowledgement tended to deter bullying while shame displacement predicted bullying (Ahmed et al., 2006). Because shame is self-imposed embarrassment or the loss of self-respect when a bad behavior is acknowledged and responsibility for the behavior is asserted, it is likely that shame will contribute to the deterrent effects of the sanction construct.

Deterrence theory provides the rationale for proposing that sanctions will have a significant effect on the commission of deviant behavior. In our model, formal sanctions, informal sanctions and shame comprise two higher-order constructs: the certainty and the severity of sanctions, which are conceptually distinct (Blumstein et al., 1978; Straub, 1990). Certainty of sanctions represents the likelihood that the delinquent would experience penalties whereas sanction severity

relates to how the penalties would negatively affect the delinquent's life (Straub, 1990, Siponen & Vance, 2010). Indeed, when there is a high risk of punishment (sanction certainty) and the punishment is harsh (sanction severity), deterrence theory postulates that the deviant act is less likely to occur. The distinctiveness of certainty and severity has been demonstrated in the IS literature with the finding that sanction severity had a greater explanatory effect on computer abuse compared to sanction certainty (Straub, 1990). Taken together, the above discussion leads to the following two hypotheses:

Hypothesis 2 (H2): Certainty of Sanction is negatively associated with intentions to cyberbully in Facebook.

Hypothesis 3 (H3): Severity of Sanction is negatively associated with intentions to cyberbully in Facebook.

Control Variables

Previous literature reports mixed results regarding the gender effects of cyberbullying. For example, it has been reported that men and women were equally likely to be involved in online harassment either as the perpetrator or the target of cyberbullying (Slonje and Smith, 2008). However, other research indicates that females are more likely to bully others online compared to their male counterparts (Li, 2006). Kernaghan and Elwood (2013) suggest that girls prefer to use indirect ways to bully others and the cyber world has provided them a "hidden" stage to do it. Thus, we include gender as a control variable.

Research also indicates that time spent online is an antecedent of cyberbullying (Gorzig & Frumkin, 2013) and the intensity of Facebook use is positively related to cyberbullying (Kwan & Skoric, 2013). Thus, Facebook involvement is included as an additional control variable. The four measures of Facebook involvement were derived from the measures of Facebook intensity (Ellison, Steinfield, & Lampe, 2007). Each item is an attitudinal question designed to measure the participant's daily and emotional connection with Facebook and sense of belonging to Facebook.

Research Design

Social desirability bias was a significant concern in the conduct of our study. Social desirability is the need for social approval and acceptance by others that is directly related to one's acceptable and appropriate behaviors (Crowne & Marlowe, 1964). Individuals tend to hide their true feelings about a controversial or self-implicating issue or topic so as to present themselves in a socially acceptable way. Hence, in measuring one's intention to cyberbully, the concept of social

desirability posits that the individual would tend to hide intentions to act offensively in order to present a socially acceptable persona. This tendency is problematic, not only because of its potential to bias the answers of respondents about 'Intentions to Cyberbully in Facebook', but also because it may mask the true relationships between two or more variables (Ganster, Hennessey, & Luthans 1983). Researchers have noted that social desirability can produce spurious relationships, mask true relationship, or influence the nature of the relationships among variables (Ganster et al., 1983). Hence, the research design discussed below was constructed in order to hinder social desirability bias.

Scenario Design

We empirically assessed our model using a hypothetical scenario method (Weber, 1992). This technique uses vignettes that contain written descriptions of realistic situations involving fictitious characters which are presented to the research subjects. The subjects are then asked to disclose their tendency to commit the same behavior as the scenario character on a number of rating scales that measure the dependent variables of interest (Trevino, 1992; Siponen & Vance, 2010). Scenario-based methods are a common means of assessing antisocial and unethical behaviors in situations where respondents tend to hide their true intentions to commit those behaviors (Pogarsky, 2004). Fifty-five percent of 174 ethical decision-making articles in premier business journals employed a scenario methodology (O'Fallon & Butterfield, 2005).

Siponen and Vance (2010) highlight two vital points in designing hypothetical scenarios. First, the scenarios must be commonplace situations that would be realistic to the respondents (Piquero & Hickman, 1999). Our design includes activities in which the scenario characters "comment on another's Facebook page" and "upload a picture." These are both commonplace Facebook activities and a means by which cyberbullying occurs in Facebook. Commenting on another's Facebook page is the most common Facebook activity and uploading a picture, while also common, is considered an especially negative way to cyberbully (Smith et al., 2008, Sticca & Perren, 2013). Second, specific details such as names of persons and companies should be mentioned in the cases (Piquero & Hickman, 1999). In keeping with these points, two scenarios were developed with different settings, a company setting and a college setting, and different levels of severity. Additionally, research indicates that females tend to cyberbully indirectly via rumors and nonverbal content such as pictures (Besag, 2006; Kernaghan & Elwood, 2013). Thus, the two scenarios differed by gender with a male perpetrator in

scenario 1 and a female perpetrator in scenario 2. Table 1 illustrates the design of the scenarios which are presented in Appendix A.

Table 1. Scenario Design

Scenario Characteristics	Scenario 1	Scenario 2
Activity	Comment on another's Facebook page	Upload a picture
Setting	Company setting	College setting
Severity	Low severity	High severity
Perpetrator	Male	Female

Measures

Most of the construct items were adopted from previously validated instruments and measured on a 7 point Likert-type scale. The denial of responsibility and denial of injury items were based on the definitions from Sykes and Matza (1957), adopted from Siponen and Vance (2010) and adapted to the Facebook context of the study. The denial of victim items originated with Sykes and Matza (1957), were used by Cromwell and Thurman (2003) and adapted to the Facebook context. The formal sanctions items of Nagin and Paternoster (1993) were modified to include actual Facebook sanctions #15 or #5.5 from the "Statement of Rights and Responsibilities" (Facebook, 2012). The informal sanctions items were derived from Nagin and Paternoster (1993). Shame reflects both the risk and cost of the perceived punishment (Nagin & Paternoster 1993) and differs in accordance with severity and certainty conditions (Siponen & Vance, 2010). The dependent variable, Intention to Cyberbully in Facebook, was measured using two items. One item was adapted from Siponen and Vance (2010) and states, "What is the chance that you would do what [the scenario character] did in the described scenario?" The other item was created to avoid the reliability threat from using a single measure (Cook & Campbell 1979). All measurement items and their descriptive statistics are included in Appendix B.

Data

Data for the study were collected from a convenience sample of six undergraduate MIS classes at a large southwestern university in the U.S. Most of the students (86.8%) were in the 18-20 age range which is representative of both Facebook users and young adults that will soon enter the workforce with undergraduate degrees. We collected data for each class in an electronic classroom in which all students could access the internet. The instructor of each class provided the survey link to the students, participation was voluntary, and no class credit or other incentive was provided for participation. Out of 270 total

students, 174 responded to the survey providing a response rate of 64.4 percent. U.S. college students make a compelling sample for investigating cyberbullying in Facebook because they make up a large percentage of Facebook users (32.8%) (ISL, 2011) and tend to devote significant time to Facebook (101.93 minutes/day) (Junco, 2011; Adkins, 2013). A link to one of the two scenarios was randomly assigned to each of the potential participants. The completed surveys were fairly evenly divided among gender. Interestingly, about 59 percent of the respondents indicated having more than 400 Facebook friends. Table 2 summarizes the demographic information of the respondents.

Table 2. Respondent Demographics

Characteristics		Number	Percentage
Gender	Male	86	49.4%
	Female	88	50.6%
Age	18	62	35.6%
	19	62	35.6%
	20	27	15.3%
	>20	23	13.2%
Number of Facebook Friends	1-100	10	5.7%
	101-200	17	9.8%
	201-300	26	15.0%
	301-400	19	10.9%
	>400	102	58.6%
Minutes per day on Facebook	31-60	36	20.7%
	1-2 hours	27	15.5%
	2-3 hours	12	6.9%
	>3 hours	11	6.3%

Sample Size

In PLS-SEM, sample size is an important consideration to achieve the power necessary to detect relationships in the model. Using the method of Cohen (1992), achieving statistical power of 80 percent and minimum R² of .10 in the dependent variable (intention to cyberbully) at a 5 percent significance level would require a sample size of 166. Our sample size of 174 indicates that statistical power of 80 percent is achieved.

Model Analysis

The three higher-order constructs (Neutralization, Certainty, Severity) are modeled as a formative second-order latent variables using the repeated indicator approach (Wold, 1985; Becker, Klein & Wetzels, 2012) because the three first-order constructs for each are reflective (Hair et al., 2014). This modeling approach is used in order to estimate all

constructs simultaneously and enhance the interpretability of the nomological network (Becker, et al., 2012). The repeated indicator approach is also appropriate because the first-order constructs have an equal number of indicators (Chin, Marcolin, & Newsted, 2003) and is recommended for reflective-formative hierarchical models as it results in more precise estimates of parameters and a more reliable second-order construct score (Becker et al., 2012).

The research model was analyzed using SmartPLS (Ringle, Wende, & Becker, 2014), a Partial Least Squares (PLS) Structural Equation Modeling (SEM) tool. PLS-SEM simultaneously assesses the psychometric properties of the measurement model and estimates the parameters of the structural model. We chose an SEM technique to test our research model because of the multi-dimensional nature of our constructs and because PLS-SEM enables the specification of second-order molar constructs that follow the logic of formative factors (Chin & Gopal, 1995). Additionally, PLS-SEM works well for small sample sizes (Chin & Newsted, 1999) and was intended to aid the 'discovery-oriented' or theory development process (Wold, 1985) for research such as ours in which the theory underlying cyberbullying behavior is in the exploratory stage.

Measurement Model

A 5000 bootstrap resampling of the data was performed as recommended (Hair et al., 2014). The reflective measures in the model were assessed based on item reliability, construct reliability, convergent validity and discriminant validity. Construct reliability was evaluated using Cronbach's alpha and composite reliability (CR) (Roldan & Sanchez-Franco, 2012). As shown in Table 3, all measures exceeded the recommended threshold value of 0.70 (Nunnally, 1978) with Cronbach's alpha ranging from 0.77 to 0.96 and CR ranging from 0.86 to 0.97. Convergent validity was assessed using average variance extracted (AVE) with values of 0.50 or more indicating that the construct accounts for at least half of its item's variance (Chin, 1998). AVE values ranged from 0.60 to 0.92, all greater than the recommended threshold. Table 4 reports the construct correlations with the bolded elements on the matrix diagonal representing the square root of each construct's AVE.

Discriminant validity was evaluated using measurement item loadings and cross-loadings, the Fornell-Larcker criterion and the heterotrait-monotrait (HTMT) ratio.

Table 3. Reliability and Validity of Reflective Items

Reflective Constructs	Item	Item Loading	Loading t-value	AVE	CR	Cronbach's alpha
Denial of Responsibility	DR1	0.933	46.023	0.90	0.97	0.95
	DR2	0.969	99.175			
	DR3	0.949	67.705			
Denial of Injury	DI1	0.946	66.150	0.86	0.95	0.92
	DI2	0.884	27.013			
	DI3	0.957	86.363			
Denial of Victim	DV1	0.943	67.871	0.90	0.97	0.95
	DV2	0.939	65.813			
	DV3	0.965	118.730			
Formal Sanction Certainty	FSC1	0.939	62.535	0.89	0.96	0.94
	FSC2	0.961	82.441			
	FSC3	0.927	58.695			
Informal Sanction Certainty	ISC1	0.940	76.407	0.83	0.94	0.90
	ISC2	0.895	46.463			
	ISC3	0.901	42.436			
Shame Certainty	SC1	0.944	30.886	0.88	0.96	0.93
	SC2	0.959	92.187			
	SC3	0.904	51.807			
Formal Sanction Severity	FSS1	0.933	80.817	0.92	0.97	0.96
	FSS2	0.984	344.904			
	FSS3	0.960	136.874			
Informal Sanction Severity	ISS1	0.931	71.108	0.80	0.93	0.88
	ISS2	0.917	58.061			
	ISS3	0.840	32.066			
Shame Severity	SS1	0.967	48.095	0.92	0.97	0.96
	SS2	0.967	138.433			
	SS3	0.940	150.251			
FB Involvement (control variable)	FB1	0.661	2.353	0.60	0.86	0.80
	FB2	0.784	3.468			
	FB3	0.765	2.977			
	FB4	0.875	4.099			
Intentions	Int1	0.870	25.506	0.81	0.90	0.77

Table 4. Latent Variable Correlations and Fornell-Larcker Criterion

	DI	DR	DV	FSC	ISC	SC	FSS	ISS	SS	FB	Gender	Intent
DI	0.930											
DR	0.702	0.950										
DV	0.822	0.732	0.949									
FSC	0.015	-0.023	-0.020	0.943								
ISC	-0.248	-0.290	-0.317	0.417	0.912							
SC	-0.455	-0.483	-0.458	0.009	0.340	0.936						
FSS	-0.077	-0.033	-0.132	0.127	0.133	0.136	0.959					
ISS	-0.381	-0.256	-0.387	0.005	0.415	0.474	0.469	0.897				
SS	-0.434	-0.534	-0.448	0.137	0.424	0.678	0.140	0.466	0.958			
FB Inv	-0.066	-0.103	-0.090	-0.069	0.102	0.163	0.433	0.190	0.033	0.775		
Gender	0.024	0.000	0.020	0.138	0.005	0.019	0.083	0.065	-0.028	0.101	1.000	
Intention	0.466	0.497	0.488	-0.178	-0.437	-0.233	0.060	-0.184	-0.387	0.095	-0.064	0.900

DI = Denial of Injury; DR = Denial of Responsibility; DV = Denial of Victim; FSC = Forman Sanction Certainty; ISC = Informal Sanction Certainty; SC = Shame Certainty; FSS = Formal Sanction Severity; ISS = Informal Sanction Severity; SS = Shame Severity; FB Inv = Facebook Involvement .

Table 5. HTMT Results

	DV	DI	DR	FSC	ISC	SC	ISS	SS
DI	.87 [.802;.942]							
DR	.77 [.659;.865]	.75 [.617;.872]						
FSC	-.02 [.181;.123]	.02 [.148;.169]	-.02 [.157;.121]					
ISC	-.34 [.463;.215]	-.27 [.395;.152]	-.32 [.442;.203]	.45 [.336;.581]				
SC	-.49 [.623;.362]	-.49 [.622;.355]	-.51 [.646;.378]	.01 [.165;.185]	.37 [.255;.512]			
ISS	-.43 [.566;.267]	-.42 [.561;.281]	-.28 [.428;.141]	.01 [.160;.162]	.47 [.293;.619]	.52 [.386;.640]		
SS	-.47 [.603;.336]	-.46 [.613;.326]	-.56 [.678;.437]	.14 [.010;.290]	.45 [.338;.588]	.72 [.554;.855]	.50 [.338;.667]	
FSS	-.14 [.276;.010]	-.08 [.209;.044]	-.03 [.154;.097]	.14 [.019;.286]	.14 [.029;.302]	.14 [.028;.309]	.51 [.306;.638]	.15 [.029;.318]

The table of loadings and cross loadings in Appendix C shows that each reflective item loads highest on its assigned construct (0.76 to 0.98) with lower loadings on all other constructs. The Facebook involvement items represent a control variable and loaded from 0.66 to 0.87. Two of the Denial of Injury items cross-loaded highly on the Denial of Victim construct and the difference between each loading and the high cross-loading was greater than 0.1, demonstrating an order of magnitude larger than any other loading (c.f., Gefen & Straub, 2005). Other tests were evaluated in the decision to retain all items. For example, in all cases the square root of the AVE was greater than the off-diagonal elements in their corresponding row and column, supporting discriminant validity of the latent variables (Fornell & Larcker, 1981). The heterotrait-monotrait ratio was also calculated because it is considered a more sensitive test to detect discriminant validity problems for reflectively measured items (Henseler, Ringle & Sarstedt, 2014). The recommended HTMT.90 criterion was used and the results are shown in Table 5 along with confidence intervals. The results do not indicate discriminant validity problems as each ratio is below the HTMT.90 criteria and the confidence intervals do not contain 1.0 (Henseler et al., 2014). Additionally, the exploratory nature of the research in which criminalization theory is used to model the constructs in an electronic-behavior context as well as our focus at the construct level contributed to the decision to retain all the items in the model.

Furthermore, all the weights of the formative dimensions of neutralization are significant and positive: denial of injury (.353, $t = 21.476$), denial of

responsibility (.365, $t = 30.080$) and denial of victim (.377, $t = 28.637$). Similarly, the weights between each certainty and severity dimension and its higher order construct is positive and significant. Table 6 provides a summary of the weights between each first-order and second-order construct.

The formative dimensions are expected to explain unique variance in their associated higher-order construct; therefore, a variance inflation factor test (VIF) was performed to check for indicator collinearity that would confound the interpretation of each indicator on its higher-order construct (Bollen, 1989). The VIF statistics for the certainty dimensions ranged from 1.159 to 1.402, the severity dimension VIFs ranged from 1.290 to 1.622, and the values for neutralization were 2.307 for denial of responsibility, 3.302 for denial of injury, and 3.606 for denial of victim. The denial of victim VIF was above the recommended threshold of 3.33 (Diamantopoulos & Sigua, 2006) although all were below the more liberal threshold of 5.0 (Hair et al., 2014). Multicollinearity was not considered a substantive threat to the estimation of the neutralization construct for several reasons.

The t-values of the three formative dimensions were high and significant ranging from 21.010 to 30.569 and no indicator had a low/non-significant path or a sign change that would indicate significant multicollinearity (Cenfetelli & Bassellier, 2009). Furthermore, the formative dimensions of neutralization are conceptually distinct (Sykes & Matza, 1957) and correlations are less than 0.90 (Cenfetelli & Bassellier, 2009) ranging between 0.70 and 0.82.

Table 6. Molar Second-Order Structural Weights

Second-Order Construct	First-Order Constructs	Weights	t-Value	VIF
Neutralization	Denial of Responsibility	.365	30.569	2.307
	Denial of Injury	.353	21.010	3.302
	Denial of Victim	.377	28.435	3.606
Certainty of Sanction	Formal Sanction Certainty	.422	7.166	1.241
	Informal Sanction Certainty	.569	15.458	1.402
	Shame Certainty	.383	5.728	1.159
Severity of Sanction	Formal Sanction Severity	.364	5.731	1.295
	Informal Sanction Severity	.456	16.547	1.622
	Shame Severity	.494	8.951	1.290

Structural Model Results

First, we examined the model for collinearity among the predictors of the dependent variable Intention (Hair et al., 2014). The VIF value for each predictor was below the common threshold of 5.0 (Hair et al., 2014) and 3.33 (Diamantopoulos & Sigauw, 2006) ranging from 1.017 to 1.665. Collinearity was not considered a substantive problem in the research model.

The PLS model results are depicted in Figure 2. A summary of the structural model results are in Table 7. As predicted, H1 is supported in that neutralization is significantly and positively related to intentions to cyberbully (.474, $p < .001$). H2 is also supported because the certainty of sanctions is significantly and negatively related to intentions to cyberbully (-.286, $p < .001$). Unexpectedly, the relationship in H3 between the severity of sanctions and intentions to cyberbully was not significant (.080, $p > .05$). Overall, the higher-order constructs account for 36.8% of the variance ($R^2 = 0.368$) in intentions to cyberbully. More specifically, neutralization accounts for 21.2% of the variance while certainty accounts for 11.9% and severity accounts for 3.5% respectively.

The effect size (f^2) of neutralization, certainty and severity were determined to assess the substantive impact of each on the intentions variable. The effect size

computations follow Cohen (1988) in which 0.02, 0.15, 0.35 represent small, medium and large effects respectively. Neutralization had the largest substantive effect on intentions with $f^2 = 0.271$, followed by certainty ($f^2 = 0.089$) and severity with a negligible effect ($f^2 = 0.006$). The cross-validated redundancy approach using the blindfolding procedure and an omission distance of 7 was used to estimate the predictive relevance Q^2 of the model. The Q^2 value is 0.267 and because it is larger than zero implies that the model has predictive relevance with regard to the reflective endogenous construct Intentions (Hair et al., 2014). The q^2 effect sizes for neutralization, certainty and severity were also determined. The q^2 effect of neutralization on intentions is 0.18, certainty on intentions is 0.05, and severity on intentions is negligible at 0.001. Using the values of 0.02, 0.15, and 0.35 small, medium and large (Cohen, 1988), neutralization has moderate predictive relevance on the dependent variable intentions while certainty demonstrates a small amount of predictive relevance.

Prior research indicates that gender may play an explanatory role in cyberbullying. Additional ad-hoc analysis was performed to consider the effect of gender on the model's paths. The data set was divided into male (N = 86) and female groups (N = 88) and each group was subjected to a 5000 bootstrap resampling and multi-group analysis (MGA) in SmartPLS. PLS-MGA represents recent developments for testing group differences and several approaches have been proposed (Sarstedt, Henseler & Ringle 2011). We tested for differences in the hypothesized paths between males and females using the permutation-based approach (Sarstedt et al., 2011). As shown in Table 8, there was no indication that the model's paths differed significantly between the male and female respondents under this approach.

Discussion

Theoretical Implications

Our research study has several theoretical contributions. First, the formative nature of the three second-order constructs lends parsimony to the theoretical underpinnings of neutralization and deterrence which were jointly used to model cyberbullying behavior. The second-order formative constructs (neutralization, certainty, severity) enable us to consider the nomological framework of deterrence at the construct level, rather than at the individual measurement level.

Thus, the model demonstrates that neutralization (.474) is an effective enabler of deviant behavior and occurs prior to the behavior as suggested in the literature (Sykes & Matza, 1957). Additionally, within the framework of deterrence our model implies that counteracting neutralization techniques would serve to deter deviant behavior.

Table 7. Results of Structural Model Paths

Hypotheses	Path Coeff	Std Error	*t-Stat	95% CI	Hypo Results	f ²	q ²
H1(+): Neutralization → Intention	0.474	0.091	5.185	[0.323, 0.625]	Supported	0.271	0.180
H2(-): Certainty → Intention	-0.286	0.087	3.299	[-0.429, -0.143]	Supported	0.089	0.050
H3(-): Severity → Intention	0.080	0.088	0.906	[-0.066, 0.225]	Not Supported	0.006	0.001
Gender → Intention (control)	-0.071	0.060	1.185	[-0.169, 0.028]	N/A	0.008	N/A
FB Involvement → Intention (control)	0.153	0.071	2.162	[0.036, 0.269]	N/A	0.034	N/A

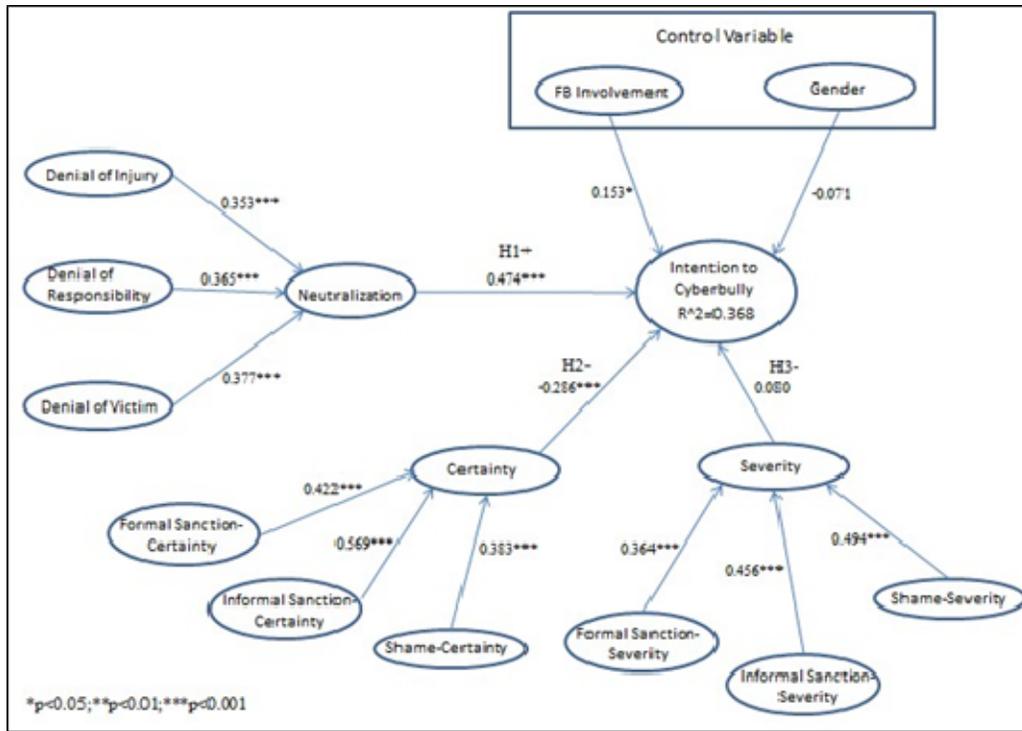


Figure 2. Structural Model

Table 8. Structural Path Differences by Gender

Path	Group	Coeff.	Bias-Corrected Confidence Intervals	Std Err	*t-stat	Permutation-Based Approach
						Path Diff
H1: Neutralization → Intention	Male	0.604	[.364;.801]	0.112	5.382 p=.000	0.268 p =0.129 No Diff
	Female	0.336	[.035;.623]	0.147	2.292 p=.023	
H2: Certainty → Intention	Male	-0.174	[-.386;.084]	0.129	1.355 p=0.177	0.205 p =0.219 No Diff
	Female	-0.379	[-.621;-.157]	0.120	3.158 p=.002	
H3: Severity → Intention	Male	0.156	[-.104;.407]	0.137	1.140 p=.256	0.187 p =0.212 No Diff
	Female	-0.031	[-.278;.264]	0.153	0.201 p=.841	

Neutralization is shown to support the intention to cyberbully with little relative difference in the specific contributions of the three dimensions. Because the weight of an indicator is useful for evaluating the importance of a construct's formative measures (Cenfetelli & Bassellier, 2009), the denial of victim dimension (.377) shows a greater contribution to the neutralization construct relative to denial of responsibility (.365) or denial of injury (.353) in our model.

Additionally, we modeled the certainty and severity of sanctions as independent formative constructs that were expected to have significant inhibiting effects on cyberbullying behavior. These constructs are also higher-order latent variables comprised of three specific dimensions. The model results demonstrate the distinctiveness of the certainty and severity constructs and their composite dimensions. For example, the facet of certainty tested as informal sanctions is more influential (.569) compared to formal sanctions certainty (.422) or shame certainty (.383). Unexpectedly, at the higher-order level, perceptions of the severity of sanctions were ineffective to inhibit deviant behavior compared to the certainty of sanctions. This finding is corroborated in criminological research which suggests that the severity of a sanction has less effect on crime deterrence compared to the certainty of a punishment (Wright, 2010). Thus, we suggest that the two significant relationships (H1: neutralization and H2: certainty of sanctions) implies a tension in which cyberbullying behavior may be explained in terms of both enabling and deterring factors. The ability of the cyberbully to rationalize or eliminate the association between his/her behavior and personal responsibility, the reality of a victim or an injury enables the behavior. In contrast, the concreteness and guarantee of sanctions is an effective deterrent.

Within the framework of deterrence, our study suggests that it is plausible to consider the role of specific structural characteristics of social networks that may enable neutralization or inhibit sanctions. For example, the asynchronous nature and/or intangibility of social network communications may enable an individual to effectively detach himself from a bad behavior and/or the consequences of the behavior. This disconnect appears to enable neutralization defenses and may render sanction deterrents ineffective. Additionally, structural SNS traits that allow greater transparency and reporting mechanisms that identify offenses and offenders may strengthen the efficacy of sanctions. Further studies that examine this tension within a framework of deterrence and the structural attributes of social networks would advance the understanding of this antisocial phenomenon.

Practical Implications

Neutralization

In the process of neutralization, denying the victim essentially eliminates the risk that another user could claim 'victimhood' after experiencing cyberbullying behavior. When the existence of a victim is denied, the perpetrator may be playing the role of the avenger (Sykes & Matza, 1957) who metes out justice. In this case, the cyberbully may have (in his own mind) successfully altered the victim's character into that of a wrong-doer. Thus, it would be rational for a Facebook user that denies a victim to post a derogatory comment or compromising picture if another user 'deserves it.'

Furthermore, the denial of responsibility is an orientation that deflects blame for violating a social norm and the delinquent may place blame on his environment. For example, if the online community is one in which users tend to spread gossip the cyberbully may be convinced that he is not responsible because such behavior has occurred in the past and is likely to occur again. Similarly, in denial of injury the restraining influences on bad behavior are undermined when an injury is not acknowledged because 1) it is not physical, 2) it is not illegal, and/or 3) it does not cause great harm. If the injury is separated from its injuriousness, then it may be rationalized as a prank in an attempt to qualify it as normative. In denying responsibility and injury, the cyberbully has rationalized the outcome prior to the action and is more likely to commit the offense.

Sociologists suggest that when a victim is physically absent from an attack (e.g., property damage) an awareness of the harm to the victim is diminished (Sykes & Matza, 1957). The nature of the online environment may contribute to injury denial due to the lack of physical proximity between the cyberbully and the victim. Future research to clarify how the mechanisms of neutralization function relative to physical proximity among the parties in cyberbullying would advance our understanding of the implications of cyberbullying behavior in organizations where greater physical proximity may exist in work-related contexts. Additionally, it would be prudent to examine how SNS users perceive psychological harm versus physical harm and the implications each might have on employee satisfaction and productivity.

Neutralization techniques are ineffective in controlling behavior because they precede rather than follow anti-social behaviors (Sykes & Matza, 1957). Our research model demonstrates that neutralization is employed prior to the commission of cyberbullying. Thus, diminishing the influence of neutralization should occur prior to the behavior. Because the cyberbully tends to disassociate him/herself from the behavior, the victim,

and the injury, it would be important to re-establish those relationships. We suggest that neutralization tendencies would be minimized by reinforcing the relationship between 1) the cyberbully's action and the victim, 2) the cyberbully and the behavior and 3) the cyberbully's action and the psychological or physical harm. Sociologists argue that interpretations of responsibility are cultural constructs not internally derived (Sykes & Matza, 1957). Therefore, societal forces must be involved in strengthening the linkages that are severed by neutralization techniques in order to reduce the opportunity for neutralization to encourage bad online behavior. Interestingly, it has been suggested that one's learning of neutralization techniques, rather than an ignorance of social norms, is key to delinquency (Sykes & Matza, 1957). This implies that, without adequate deterrents, cyberbullying behavior is likely to continue; not because SNS users are ignorant of societal norms, but because the norms may be intentionally and effectively neutralized.

Sanctions

Sanctions or punishment are often proffered as a means to control behavior by delineating the consequences that would be meted out for infractions to stated policies. In our study, the certainty of sanctions occurring was a more formidable deterrent than consideration of the severity of the sanctions. We surmise that individuals may consider the inevitability of punishment of greater import than severity in the decision to cyberbully because certainty may represent a kind of guarantee that a penalty is inescapable. If a sanction is unavoidable then the certainty of it occurring is high, whereas a severe sanction may not convey the idea of unavoidability that would prompt immediate scrutiny. Research in criminology indicates that punishment severity has little effect on crime deterrence compared to increasing the certainty of the punishment (Wright, 2010). At the construct level, our study appears to support this notion in the context of cyberbullying as well.

The dimension contributing most to the certainty construct is the certainty of informal sanctions, followed by the certainty of formal sanctions. Informal sanctions represent the idea that others will be informed of one's cyberbullying behavior. It appears that emphasizing the certainty of this outcome is a useful means to reinforce the inevitability of a detrimental consequence. This effect may result from the innate characteristics of SNSs like Facebook where the bullying activity may be visible to the community of users who are 'friends' with the victim. In face-to-face bullying and text message bullying, the activity is more restricted in terms of being observed by others. In contrast, a more open SNS

community like Facebook generally allows one's approved 'friends' to view others' messages with immediate and unhindered access. Facebook users know that their messages posted to another's 'wall' are not anonymous and may be widely read. Thus, the risk of disapproval by others for an offensive message may be higher than in other types of digital communications. The technical structure of the SNS may play a role in deterring offensive behavior if there is openness and a lack of anonymity. It would be useful for future research to examine how technical structures of social media platforms may inhibit cyberbullying. For example, community openness and transparency as well as reporting mechanisms would reinforce the certainty the others will know of one's SNS behavior.

Facebook has recently implemented an anti-cyberbullying program that recognizes the effectiveness of informal deterrents. This new reporting feature is available only for a community of 'trusted friends' and will allow cyberbullying victims to report offensive content as well as alert someone (e.g., parents, teachers) in their support system so that online activities are allied with 'real world' consequences. Organizational SNSs created for employees and customers should recognize that deterrents are critical to control offensive behavior, prevent the loss of users and customers, and protect their brand.

Limitations and Future Research

This study, although insightful, is not free of limitations. The first limitation lies in the sample. Individuals aged 10 to 20 may be the most vulnerable to cyberbullying activity; however, our sample was composed primarily of young adults aged 18 to 20. Thus, an important component of the population of Facebook users (i.e., children and teens) involved with offensive online behavior was not included in the study. Although the respondents in our study represent young adults (i.e., college students and employees) who are SNSs users, this was primarily a convenience sample. Future researchers are encouraged to test the model in larger samples of college-age students as well as among employees that utilize SNSs in the organization. Although the convenience sample limits the generalizability of the results, it is likely that we have captured the attitudes and perceptions of social media users who will soon become organizational employees with access to social media in the organization as well as in the greater community of SNS users. Because Facebook is the current leader in social networking, our respondents have provided insight that is valuable for other social media with similar communication and interaction capabilities. However, it would be useful to examine the model's relationships among other types of SNSs and with various ages of users to understand

how neutralization processes and deterrents may differ among SNSs and users.

The use of intention as the dependent variable raises the question as to whether or not intention is indicative of actual behavior. Intention has been recognized as a valid proxy for behavior in IS research from the beginning of the implementation of the Theory of Planned Behavior that explored the relationship between intention and actual behavior, underpinning the strong correlation between the two variables (Fishbein & Ajzen, 1975). Future researchers might attempt to measure actual behavior to increase the model's validity. The effect of social desirability bias will always be a limitation in studies of this nature in which respondents report on behaviors of an offensive nature. Even though the use of scenarios depicting the actions of others is a valid attempt to hinder this bias, the degree to which true intentions were reported is unknown. Future researchers should include additional remedies for this bias in the design and operationalization of cyberbullying models.

Our study highlights several directions for future research in this area. For example, experimental studies are needed to demonstrate the causal effect of neutralization on compliance/noncompliance to cyberbullying policies, possibly comparing the effects of neutralization vis-à-vis those of sanctions. Second, in both survey and experimental designs, future research could also explore the boundary conditions associated with employing neutralization techniques. Why might SNS users choose to justify or rationalize offensive online behavior in some situations but not in others? What types of formal and informal sanctions are more/less effective in deterring cyberbullying in organizational SNSs?

Conclusion

The old adage "with a friend like that, who needs enemies" takes on new meaning in SNSs as a network "friend" can become a cyberbully with the click of a mouse. The objective of our study was to clarify the antecedents of cyberbullying behavior in terms of a nomological framework incorporating neutralization and deterrence. Our theoretical and empirical insights lead to several key contributions. In answer to the research question of why cyberbullying might occur in SNSs among young adults, we found that neutralization processes play a significant role in enabling the behavior. Rationalizing one's responsibility for cyberbullying and/or severing the link between the behavior and a victim or the behavior and an injury explains why users may participate in offensive online behavior. Additionally, the empirical results indicate that the certainty of sanctions may be an effective inhibitor of cyberbullying while sanction severity offer little to deter the cyberbully. At

the practical level, the challenge for SNSs is to develop methods or means to specifically counteract the neutralization processes related to denials of victim, responsibility and injury as well as increase the certainty of sanctions. Further research is required to identify the online behaviors that are likely to be carried into the organization by young adults who have been using SNSs for years - for the protection of both employees and organizations.

References

- Adkins, S. (2013). *Wealthier College Students Spend More Time on Facebook: Study*. UNIVERSITY HERALD, 06/26/2013 (<http://www.universityherald.com/articles/3670/20130626/wealthier-college-studentsspend-more-time-Facebook-study.htm#>)
- Ahmed, E., Harris, N., Braithwaite, J., and Braithwaite, V. (2001). *Shame management through reintegration*. Press, Melbourne, Cambridge University.
- Ahmed, E., Harris, N., and Braithwaite, V. (2006). "Forgiveness, Reconciliation, and Shame: Three Key Variables in Reducing School Bullying." *Journal of Social Issues*, Vol. 62, No. 2: pp. 347-370.
- Badiuk, B. (2006). *Cyberbullying in the global village: The worldwide emergence of high-tech as a weapon for bullies*. In A. Green (Ed.), *Education students' anthology* (Vol. 9) (pp.12-16). Winnipeg, MB: Faculty of Education.
- Bastiaensens, S., Vandebosch, H., Poels, K. Van Cleemput, K., DeSmet, A., and De Bourdeauhuij, (2014). "Cyberbullying on social network sites. An experimental study into bystanders' behavioral intention to help the victim or reinforce the bully." *Computers in Human Behavior*, Vol. 31: pp. 259-271.
- Becker, J., Klein, K., and Wetzels, M. (2012). "Hierarchical latent variable models in PLS-SEM: guidelines for using reflective formative type models." *Long Range Planning*, Vol. 45: pp. 359-394.
- Besag, V. (2006). *Understanding girls' friendships, flights and feuds: A practical approach to girls' bullying*. Maidenhead England: New York: Open University Press.
- Blumstein, A., Cohen, J., and Nagin, D. (1978). "Introduction" in *Deterrence and Incapacitation: Estimating the Criminal Effects of Criminal Sanctions on Crime Rates*. National Academy of Sciences, Washington, D.C.. Editors: Blumstein, A., Cohen, J., and Nagin, D.
- Bollen, D. (1989). *Structural Equations with Latent Variables* (1st ed.), Wiley-Interscience, Malden, MA.
- Boyd, D., and Ellison, N. (2007). "Social Network Sites:

- Definition, History, and Scholarship." *Journal of Computer-Mediated Communication*, Vol. 13, No. 1: pp. 210–230. Broucek, F. (1991). *Shame and the Self*. Guilford Press, New York.
- Cao, L. (2004). *Major Criminological Theories: Concepts and Measurement*. Wadsworth Publishing, Belmont, CA.
- Cassidy, W., Faucher, C., and Jackosn, M. (2013). "Cyberbullying among youth: A comprehensive review of current international research and its applications and application to policy and practice." *School Psychology International*, Vol. 34, No. 6: pp. 575-612.
- Cenfetelli, R., and Bassellier, G. (2009). "Interpretation of formative measurement in information systems research." *MIS Quarterly*, Vol. 33, No. 4: pp. 689-707.
- Chin, W. (1998). "Issues and Opinions on Structural Equation Modeling." *MIS Quarterly*, Vol. 22, No.1: pp. vii-xvi.
- Chin, W., and Gopal, A. (1995). "Adoption intention in GSS: Relative importance of beliefs," *The DATA BASE for Advances in Information Systems*, Vol. 26, No. 2: pp. 42-63.
- Chin, W., and Newsted, P. (1999). *Structural equation modeling analysis with small samples using partial least squares*, in Hoyle, R. (ed.), *Statistical Strategies for Small Sample Research*, Sage, Thousand Oaks: pp. 307-341.
- Chin, W., Marcolin, B., and Newsted, P. (2003). "A Partial Least Squares Latent Variable Modeling Approach for Measuring Interaction Effects: Results from a Monte Carlo Simulation Study and an Electronic Mail Emotion/Adoption Study." *Information Systems Research*, Vol. 14, No. 2: pp. 189-217.
- Chui, M., Manyika, J., Bughin, J., Dobbs, R., Roxburgh, C., Sarrazin, H., Sands, G., and Westergren, M. (2012). *The social media economy: Unlocking value and productivity through social technologies*. McKinsey Global Institute. (http://www.mckinsey.com/insights/high_tech_telecoms_internet/the_social_economy)
- Cohen, J. (1988). *Statistical power analysis for the behavioral sciences*. Lawrence Erlbaum, Mahwah, NJ.
- Cohen, J. (1992). "A power primer." *Psychological Bulletin*, Vol. 112: pp. 155-159.
- Cook, T., and Campbell, D. (1979). *Quasi Experimentation: Design and Analytical Issues for Field Settings*. Rand McNally, Chicago.
- Cromwell, P., and Thurman, Q. (2003). "The devil made me do it: use of neutralizations by shoplifters." *Deviant Behavior*, Vol. 24, No. 6: pp. 535–550.
- Crowne, D., and Marlowe, D. (1964). *The approval motive: Studies in evaluative dependence*. Wiley, New York.
- Diamantopoulos, A. (2011). "Incorporating formative measures into covariance-based structural equation models." *MIS Quarterly*, Vol. 35, No. 2: pp. 335-358.
- Diamantopoulos, A., and Siguaw, J. (2006). "Formative versus reflective indicators in organizational measure development: a comparison and empirical illustration." *British Journal of Management*, Vol. 17, No.4: pp. 263-282.
- Dobson, S. (2012). "Cyberbullying can be harsher than other forms of workplace bullying: Study." *Canadian HR Reporter*, Vol. 25, No. 21: pp. 9-10.
- Dooley, J., Pyżalski, J., and Cross, D. (2009). "Cyberbullying versus face-to-face bullying: A theoretical and conceptual review." *Zeitschrift für Psychologie/Journal of Psychology*, Vol. 217, No. 4: pp. 182-188.
- Edwards, J. (2001). "Multidimensional constructs in organizational behavioral research: an integrative analytical framework." *Organizational Research Methods*, Vol. 4, No. 2: pp. 144-192.
- Eliason, S., and Dodder, R. (1999). "Techniques of Neutralization Used by Deer Poachers in the Western United States: A Research Note." *Deviant Behavior*, Vol. 20, No. 3: pp. 233-252.
- Elis, L., and Simpson, S. (1995). "Informal Sanction Threats and Corporate Crime: Additive Versus Multiplicative Models." *Journal of Research in Crime and Delinquency*, Vol. 20, No. 3: pp. 233-252.
- Ellison, N.B., Steinfield, C., and Lampe, C. (2007). "The Benefits of Facebook Friends: Social Capital and College Students' Use of Online Social Network Site." *Journal of Computer-Mediated Communication*, Vol. 12: pp. 1143–1168.
- Facebook (2012). *Statement of Rights and Responsibilities*. (<https://www.Facebook.com/legal/terms>.)
- Facebook Statistics. (2014). (<http://www.statisticbrain.com/Facebook-statistics/>)
- Fishbein, M., and Ajzen, I. (1975). *Beliefs, Attitude, Intention and Behavior: An Introduction to Theory and Research*. Addison-Wesley, MA.
- Foderaro, L. (2010). *Private Moment Made Public, Then a Fatal Jump*. The New York Times (NYT),09/29/2010. (http://www.nytimes.com/2010/09/30/nyregion/30s_uicide.html).
- Fornell, C., and Larcker, D. (1981). "Evaluating structural equation models with unobservable variables and measurement error." *Journal of Marketing Research*, Vol. 18, No. 1: pp. 39-50.
- Ganster, D., Hennessey, H., & Luthans, F. (1983). "Social desirability response effects: Three alternative models." *Academy of Management Journal*, Vol. 26, No. 2: pp. 321–331.

- Gefen, D., and Straub, D. (2005). "A practical guide to factorial validity using PLS-Graph: tutorial and annotated example." *Communications of the Association for Information Systems*, Vol. 16: pp. 91-109.
- Gefen, D., Straub, D., and Boudreau, M. (2000). "Structural Equation Modeling Techniques and Regression: Guidelines for Research Practice." *Communications of the Association for Information Systems*, Vol. 4, Article. 7: pp. 1-77.
- Gorzig, A., and Frumkin, L. (2013). "Cyberbullying experiences on-the-go: When social media can become distressing." *Cyberpsychology: Journal of Psychosocial Research on Cyberspace*, Vol. 7, No. 1: article 4.
- Hair, J.F., Hult, G.T.M., Ringle, C.M., and Sarstedt, M (2014). *A Primer on Partial Least Squares Structural Equation Modeling (PLS-SEM)*, Sage, Thousand Oaks, 2014.
- Hair, J., Anderson, R., Tatham, R., and Black, W. (1998). *Multivariate Data Analysis* (5th ed.), Englewood Cliffs, NJ: Prentice Hall.
- Henseler, J., Ringle, C. and Sarstedt, M. (2014). "A new criterion for assessing discriminant validity in variance-based structural equation modeling." *Journal of the Academy of Marketing Science*. (online)
- ISL, (2011). *2011 Facebook Demographics and Statistics – Including Federal Employees and Gays in the Military*. (<http://strategylabs.com/2011/01/2011-facebook-demographics-and-statistics-including-federal-employees-and-gays-in-the-military/>).
- Jarvis, C., Mackenzie, S., and Podsakoff, P. (2003). "A Critical Review of Construct Indicators and Measurement Model Misspecification in Marketing and Consumer Research." *Journals of Consumer Research*, Vol. 30, No. 2: pp. 199-218.
- Junco, R. (2011). *Students spend a lot of time Facebooking, searching, and texting*. (<http://blog.reyjunco.com/students-spend-a-lot-of-time-facebooking-searching-and-texting>).
- Kenburby (2011). *Demographics of Facebook*. (<http://www.kenburby.com/2011/03/facebook-demographics-revisited-2011-statistics-2/>)
- Kernaghan, D., and Elwood, J. (2013). "All the (cyber) world's stage: Framing Cyberbullying as a Performance." *Journal of Psychosocial Research on Cyberspace*, Vol. 7, No. 1: article 5.
- Kiron, D., Palmer, D., Phillips, A., and Kruschwitz, N. (2012). "Social business: What are companies really doing?" *MIT Sloan Management Review*. Social Business Global Executive Study.
- Kivimaki, M., Elovainio, M., and Vahtera, J. (2000). "Workplace bullying and sickness absence in hospital staff." *Occupational and Environmental Medicine*, Vol. 57: pp. 656- 660.
- Kwan, G., and Skoric, M. (2013). "Facebook bullying: An extension of battle in school." *Computers in Human Behavior*, Vol. 29: pp. 16-25.
- Li, Q. (2006). "Cyberbullying in schools: A research of gender differences." *School Psychology International*, Vol. 27, No. 2: pp. 157–170.
- MacKenzie, S. B., Podsakoff, P. M., and Jarvis, C. B. (2005). "The Problem of Measurement Model Misspecification in Behavioral and Organizational Research and Some Recommended Solutions." *Journal of Applied Psychology*, Vol.90, No. 4: pp. 710-730.
- Marcum, C., Higgins, G., Freiburger, T., and Ricketts, M. (2013). "Exploration of Cyberbullying Victim/Offender Overlap by Sex." *Am J Crim Just*, Vol. 39: pp. 538-548.
- Mishna, F., Saini, M., and Solomom, S. (2009). "Ongoing and online: Children and youth's perceptions of cyber bullying." *Children and Youth Services Review*, Vol. 31, No. 12: pp. 1222-1228.
- Morrison, B. (2006). "School Bullying and Restorative Justice: Toward a Theoretical Understanding of the Role of Respect, Pride, and Shame." *Journal of Social Issues*, Vol. 62, No. 2: pp. 371-392.
- Nagin, D., and Paternoster, R. (1993). "Enduring Individual Differences and Rational Choice Theories of Crime." *Law & Society Review*, Vol. 27, No. 3: pp. 467-496.
- Nunnally, J. (1978). *Psychometric Theory*, 2nd ed.. McGraw-Hill, New York, NY.
- O'Fallon, M., and Butterfield, K. (2005). "A Review of the Empirical Ethical Decision- Making Literature: 1996–2003." *Journal of Business Ethics*, Vol.59, No.4: pp. 375-413.
- Paternoster, R., and Simpson, S. (1996). "Sanction Threats and Appeals to Morality: Testing a Rational Choice Model of Corporate Crime." *Law & Society Review*, Vol. 30, No. 3: pp. 549-584.
- Petter, S., Straub, D., and Rai, A. (2007). "Specifying Formative Constructs in IS Research." *MIS Quarterly*, Vol.31, No.4: pp. 623-656.
- Piquero, A., and Hickman, M. (1999). "An Empirical Test of Tittle's Control Balance Theory." *Criminology*, Vol. 37, No. 2: pp. 319- 342.
- Pogarsky, G. (2004). "Projected Offending and Implications for Heterotypic Continuity." *Criminology*, Vol. 42, No. 1: pp. 111-135.
- Quine, L. (1999). "Workplace bullying in NHS community trust: staff questionnaire survey." *British Medical Journal*, Vol.318: pp. 228-232.
- Raskauskas, J., and Stoltz, A. (2007). "Involvement in traditional and electronic bullying among adolescents." *Developmental Psychology*, Vol.43: pp. 564–575.
- Ringle, C., Wende, S., & Becker, J. (2014). *Smartpls 3. Hamburg: SmartPLS*. Retrieved from <http://www.smartpls.com>.

- Rivituso, G. (2012). "Cyberbullying: an exploration of the lived experiences and the psychological impact of victimization among college students an interpretive phenomenological analysis" *Education Doctoral Theses*, Paper 21.
- Roldan, J., and Sanchez-Franco, F. (2012). Variance-based structural equation modeling: Guidelines for using partial least squares in information systems research. In M. Mora, O. Gelman, A. Steenkamp, and M. Raisinghani (Eds.), *Research methodologies in engineering of software systems and information systems: Philosophies, methods and innovations* (pp. 193-221). Hershey, PA: Information Science Reference.
- Sarstedt, M., Henseler, J., and Ringle, C. M. (2011). "Multi-Group Analysis in Partial Least Squares (PLS) Path Modeling: Alternative Methods and Empirical Results." *Advances in International Marketing*, Vol. 22: pp. 195-218.
- Siponen, M., and Vance, A. (2010). "Neutralization: new insights into the problem of employee information systems security policy violations." *MIS Quarterly*, Vol. 34, No. 3: pp. 487-512.
- Skye, J. (2012). *Cyber Bullying Statistics. Love to Know Safety*.
(http://safety.lovetoknow.com/Cyber_Bullying_Statistics)
- Slonje, R., and Smith, P. (2008). "Cyberbullying: Another main type of bullying?" *Scandinavian Journal of Psychology*, Vol. 49, No. 2: pp.147-154.
- Smith, P., Mahdavi, J., Carvalho, M., Fisher, S., Russell, S., and Tippett, N. (2008). "Cyberbullying: Its nature and impact in secondary school pupils." *Journal of Child Psychology and Psychiatry*, Vol. 49, No.4: pp. 376-385.
- Sticca, F., and Perren, S., (2013). "Is Cyberbullying Worse than Traditional Bullying? Examining the Differential Roles of Medium, Publicity and Anonymity for the Perceived Severity of Bullying." *J Youth Adolescence*, Vol. 42: pp. 739-750.
- Straub, W. D. (1990). "Effective IS Security: An Empirical Study." *Information Systems Research*, Vol.1, No. 3: pp. 255-276.
- Suler, J. (2004). "The online disinhibition effect." *Cyber Psychology & Behavior*, Vol. 7: pp. 321-326.
- Sykes, G., and Matza, D. (1957). "Techniques of Neutralization: A Theory of Delinquency." *American Sociological Review*, Vol. 22, No. 6: pp. 664-670.
- Trevino, L. (1992). "Experimental Approaches to Studying Ethical-Unethical Behavior in Organizations." *Business Ethics Quarterly*, Vol. 2, No. 2: pp. 121-136.
- Weber, J. (1992). "Scenarios in Business Ethics Research: Review, Critical Assessment, and Recommendations." *Business Ethics Quarterly*, Vol. 2, No. 2: pp. 137-160.
- Weber, M., Ziegele, M., and Schnauber A. (2013). "Blaming the Victim: The Effects of Extraversion and Information Disclosure on Guilt Attributions in Cyberbullying." *Cyberpsychology, Behavior, and Social Networks*, Vol. 16, No. 4: pp. 254-259.
- Wold, H. (1985). "Partial Least Squares," In: Kotz, S., and Johnson, N. (eds.), *Encyclopedia of Statistical Sciences*. Wiley, NY: pp. 581-591.
- Wright, V. (2010). *Deterrence in Criminal Justice: Evaluating Certainty vs. Severity of Punishment*. The Sentencing Project, November.
- Yahoo! Finance (2012). *Number of active users at Facebook over the years*.
(<http://finance.yahoo.com/news/numberactive-users-Facebook-over-years-214600186--finance.html>)
- Zalaquett, C., and Chatters, S. (2014) *Cyberbullying in College: Frequency, Characteristics and Practical Implications*. SAGE Open Vol. 4, No. 1: pp. 1-8.

About the Authors

Sixuan Zhang is a PhD candidate of Management Information Systems at Baylor University. Sixuan earned his BA degree in Industrial Engineering in BUPT, China and then worked as a consultant for IT service development for 3 years. He got his master degree in Management Information Systems from Baylor University then began his doctorate study at Baylor University in 2012. He is currently serving as a research assistant in the MIS Department. His research interests include the Business Use of Social Media, IT User Behaviors, Emotion Impacts on IT Adoption and IT Consumerization.

Liang Yu earned his master's degree in Management Information Systems from Baylor University in 2014. He is now an Analyst at HuaTai Securities Co.,Ltd.

Robin L. Wakefield is an Associate Professor of MIS at Baylor University. She earned her PhD from the University of Mississippi and has published research in numerous journals including *Information Systems Review*, *European Journal of Information Systems*, *DATA BASE*, *Journal of Strategic Information Systems*, *Communications of the ACM*, *Information & Management*, and *Behavioral Research in Accounting*, among others. Her major research interests include behavioral intention models, human-computer interaction, technology acceptance and social media.

Dorothy E. Leidner, PhD is the Ferguson Professor of Information Systems at Baylor University and a visiting professor at the University of Lund, Sweden. Since 2005, she has had a regular summer professor appointment at the University of Mannheim, Germany. She previously served as an associate professor at INSEAD (Fontainebleau, France) and TCU (Ft Worth,

TX), and has held visiting appointments at ETH-Zurich, SMU (Dallas, TX), the University of Caen (France), and ITESM (Monterrey, Mexico). Dorothy received her BA, MBA, and PhD from the University of Texas at Austin. She has over 50 refereed publications in such journals as *MIS Quarterly*, *Information Systems Research*, *Organization Science*, and the *Journal of Management Information Systems*, among others. Dorothy serves as Editor-in-Chief of *MIS Quarterly*

Executive and Senior Editor for *Information Systems Research* and for the *Journal of the Association of Information Systems*. Previously, she served in various editorial roles including co-Editor-in-Chief of *Data Base for Advances in IS*, associate editor and senior editor for *MIS Quarterly*, associate editor for *Decision Sciences Journal*, and senior editor for the *Journal of Strategic Information Systems*.

Appendix

Appendix A: Hypothetical Scenarios

<p>Scenario 1: Commenting on another's Facebook page</p>	<p>Tom is part of a team working on a company project that is operating on a tight schedule. The team members use Facebook to communicate. John was the only person to miss an important team meeting recently. Tom posts on John's Facebook page the following: "One person on our team is a complete moron!"</p>
<p>Scenario 2: Uploading a picture</p>	<p>Emily and Brianna are classmates. Emily saw a photo in which Brianna was whispering to and smiling at Emily's boyfriend at a recent party. Emily was so mad that she uploaded a picture on her Facebook page showing Brianna dancing around three guys, holding a bottle of beer, with her dress falling off one shoulder exposing an ugly tattoo. Emily titled the picture: "Who is this Slutty Whore?"</p>

Appendix B: Measurement Items and Descriptive Statistics

Constructs		Item	Mean	SD
Intention	I1	What is the chance that you would do what [the scenario character] did in the described scenario?	1.82	1.22
	I2	How acceptable was [the scenario character]'s post?	2.03	1.24
Neutralization: Denial of Responsibility	DR1	It is OK to cyberbully if you aren't sure what is or is not cyberbullying.	1.79	1.16
	DR2	It is OK to cyberbully if cyberbullying is not explained.	1.77	1.15
	DR3	It is OK to cyberbully if you don't understand what it is.	1.75	1.10
Neutralization: Denial of Injury	DI1	It is OK to cyberbully in Facebook if no harm is done.	1.72	1.06
	DI2	It is OK to cyberbully in Facebook as long as Facebook doesn't suffer the consequences.	1.55	0.92
	DI3	It is OK to cyberbully in Facebook if no one gets hurt.	1.71	1.05
Neutralization: Denial of Victim	DV1	It is OK to cyberbully in Facebook if that person 'has it coming.'	1.74	1.11
	DV2	It is OK to cyberbully in Facebook if I am retaliating for a wrong done to me.	1.78	1.13
	DV3	It is OK to cyberbully in Facebook if the person deserves it.	1.78	1.13
Certainty: Formal sanctions	FSC1	What is the chance that you would be prohibited from using part of Facebook for	2.74	1.71
	FSC2	What is the chance that you would be prohibited from using all of Facebook for	2.43	1.62
	FSC3	What is the chance that your Facebook account would be disabled for doing what	2.27	1.61
Certainty: Informal sanctions	ISC1	What is the chance that you would lose the respect of your close friends for doing what [the scenario character] did?	4.17	1.93
	ISC2	What is the chance that you would lose the respect of your parents for doing what [the scenario character] did?	4.28	1.98
	ISC3	What is the chance that you would lose the respect of your Facebook community	4.17	1.83
Certainty: Shame	SC1	How likely is it that you would be ashamed if others knew that you cyberbullied	5.88	1.52
	SC2	How likely is it that you would be ashamed if your close friends knew that you cyberbullied in Facebook?	5.73	1.61
	SC3	How likely is it that you would be ashamed if your parents knew that you cyberbullied in Facebook?	5.96	1.52
Severity: Formal sanctions	FSS1	How much of a problem would it be if you were prohibited from using part of Facebook for doing what [the scenario character] did?	3.52	1.82
	FSS2	How much of a problem would it be if you were prohibited from using all of Facebook for doing what [the scenario character] did?	4.01	1.95
	FSS3	How much of a problem would it be if your Facebook account was disabled for	4.17	1.93
Severity: Informal sanction	ISS1	How much of a problem would it create in your life if you lose the respect of your close friends for doing what [the scenario character] did?	5.44	1.63
	ISS2	How much of a problem would it create in your life if you lose the respect of your parents for doing what [the scenario character] did?	5.65	1.57
	ISS3	How much of a problem would it create in your life if you lose the respect of your Facebook community for doing what [the scenario character] did?	4.61	1.84
Severity: Shame	SS1	How much of a problem would it be if you felt ashamed that others knew that you cyberbullied in Facebook?	5.09	1.75
	SS2	How much of a problem would it be if you felt ashamed that your close friends knew that you cyberbullied in Facebook?	5.17	1.78
	SS3	How much of a problem would it be if you felt ashamed that your parents knew	5.51	1.66
FB Involvement	FB1	Facebook is part of my everyday activity.	4.55	1.82
	FB2	I am proud to tell people I'm on Facebook.	4.36	1.40
	FB3	I feel out of touch when I haven't logged onto Facebook for a while.	3.79	1.75
	FB4	I feel I am part of the Facebook community.	4.29	1.47

Appendix C: Table of Loadings and Crossloading

DI = Denial of Injury; DR = Denial of Responsibility; DV = Denial of Victim; FSC = Forman Sanction Certainty; ISC = Informal Sanction Certainty; SC = Shame Certainty; FSS = Formal Sanction Severity; ISS = Informal Sanction Severity; SS = Shame Severity; FB = Facebook Involvement; I = Intention to Cyberbully

	DI	DR	DV	FSC	ISC	SC	FSS	ISS	SS	FB	Gender	Intent
DI1	0.946	0.704	0.821	-0.016	-0.269	-0.421	-0.074	-0.387	-0.444	-0.063	-0.019	0.483
DI2	0.884	0.579	0.689	0.040	-0.226	-0.449	-0.061	-0.332	-0.376	-0.060	0.056	0.393
DI3	0.957	0.668	0.776	0.021	-0.196	-0.403	-0.080	-0.342	-0.389	-0.062	0.036	0.420
DR1	0.631	0.933	0.677	-0.082	-0.307	-0.427	-0.047	-0.223	-0.503	-0.057	0.022	0.457
DR2	0.677	0.969	0.701	0.019	-0.261	-0.465	0.003	-0.231	-0.488	-0.114	-0.008	0.467
DR3	0.691	0.949	0.708	-0.005	-0.260	-0.483	-0.050	-0.276	-0.530	-0.122	-0.013	0.493
DV1	0.801	0.659	0.943	-0.014	-0.280	-0.432	-0.129	-0.387	-0.399	-0.091	-0.003	0.429
DV2	0.763	0.701	0.939	-0.043	-0.326	-0.410	-0.100	-0.328	-0.436	-0.049	0.038	0.496
DV3	0.775	0.723	0.965	0.000	-0.298	-0.460	-0.148	-0.388	-0.441	-0.117	0.023	0.464
FSC1	-0.045	-0.057	-0.081	0.939	0.379	0.017	0.167	0.048	0.115	-0.088	0.120	-0.190
FSC2	0.033	0.033	-0.024	0.961	0.355	-0.026	0.105	-0.015	0.087	-0.112	0.086	-0.133
FSC3	0.053	-0.038	0.044	0.927	0.440	0.032	0.087	-0.019	0.182	-0.001	0.181	-0.177
ISC1	-0.245	-0.266	-0.316	0.409	0.940	0.297	0.110	0.383	0.383	0.152	0.014	-0.424
ISC2	-0.221	-0.269	-0.274	0.361	0.895	0.382	0.053	0.346	0.433	0.019	-0.063	-0.360
ISC3	-0.211	-0.258	-0.277	0.371	0.901	0.249	0.206	0.409	0.341	0.108	0.065	-0.411
SC1	-0.410	-0.443	-0.403	0.001	0.315	0.944	0.155	0.467	0.642	0.136	0.096	-0.228
SC2	-0.411	-0.450	-0.431	0.025	0.311	0.959	0.164	0.475	0.668	0.152	0.020	-0.205
SC3	-0.456	-0.462	-0.451	-0.002	0.329	0.904	0.060	0.387	0.591	0.170	-0.064	-0.222
FSS1	-0.011	0.005	-0.085	0.204	0.100	0.092	0.933	0.375	0.115	0.376	0.090	0.052
FSS2	-0.093	-0.052	-0.144	0.136	0.151	0.134	0.984	0.470	0.143	0.418	0.079	0.049
FSS3	-0.110	-0.044	-0.147	0.034	0.129	0.161	0.960	0.497	0.144	0.447	0.070	0.070
ISS1	-0.400	-0.334	-0.426	-0.031	0.383	0.470	0.395	0.931	0.450	0.133	0.043	-0.228
ISS2	-0.376	-0.211	-0.341	-0.044	0.329	0.434	0.322	0.917	0.379	0.077	0.006	-0.176
ISS3	-0.251	-0.142	-0.272	0.084	0.400	0.369	0.536	0.840	0.420	0.294	0.122	-0.091
SS1	-0.459	-0.556	-0.457	0.117	0.390	0.672	0.133	0.466	0.967	0.023	-0.020	-0.389
SS2	-0.387	-0.497	-0.443	0.164	0.440	0.657	0.170	0.463	0.967	0.026	-0.030	-0.350
SS3	-0.403	-0.480	-0.386	0.113	0.388	0.618	0.097	0.409	0.940	0.045	-0.031	-0.375
FB1	-0.134	-0.079	-0.089	-0.013	0.163	0.169	0.370	0.204	-0.002	0.661	0.088	0.022
FB2	0.020	-0.070	-0.059	-0.125	0.098	0.104	0.304	0.124	-0.029	0.784	0.075	0.076
FB3	-0.044	-0.041	0.009	0.052	0.020	0.112	0.427	0.141	0.069	0.765	0.143	0.053
FB4	-0.097	-0.117	-0.123	-0.069	0.085	0.154	0.335	0.171	0.052	0.875	0.053	0.101
Gender	0.024	0.000	0.020	0.138	0.005	0.019	0.083	0.065	-0.028	0.101	1.000	-0.064
I1	0.357	0.407	0.359	-0.065	-0.319	-0.167	0.081	-0.171	-0.263	0.099	-0.078	0.870
I2	0.470	0.481	0.502	-0.232	-0.452	-0.244	0.034	-0.163	-0.415	0.076	-0.042	0.930