This article was downloaded by: [71.245.67.81] On: 09 December 2021, At: 06:02
Publisher: Institute for Operations Research and the Management Sciences (INFORMS)
INFORMS is located in Maryland, USA

Information Systems Research

Publication details, including instructions for authors and subscription information:
http://pubsonline.informs.org

Why Do Adults Engage in Cyberbullying on Social Media? An Integration of Online Disinhibition and Deindividuation Effects with the Social Structure and Social Learning Model

Paul Benjamin Lowry, Jun Zhang, Chuang Wang, Mikko Siponen

To cite this article:
Paul Benjamin Lowry, Jun Zhang, Chuang Wang, Mikko Siponen (2016) Why Do Adults Engage in Cyberbullying on Social Media? An Integration of Online Disinhibition and Deindividuation Effects with the Social Structure and Social Learning Model. Information Systems Research 27(4):962-986. https://doi.org/10.1287/isre.2016.0671

Full terms and conditions of use: https://pubsonline.informs.org/Publications/Librarians-Portal/PubsOnLine-Terms-and-Conditions

This article may be used only for the purposes of research, teaching, and/or private study. Commercial use or systematic downloading (by robots or other automatic processes) is prohibited without explicit Publisher approval, unless otherwise noted. For more information, contact permissions@informs.org.

The Publisher does not warrant or guarantee the article's accuracy, completeness, merchantability, fitness for a particular purpose, or non-infringement. Descriptions of, or references to, products or publications, or inclusion of an advertisement in this article, neither constitutes nor implies a guarantee, endorsement, or support of claims made of that product, publication, or service.

Copyright © 2016, INFORMS

Please scroll down for article—it is on subsequent pages

With 12,500 members from nearly 90 countries, INFORMS is the largest international association of operations research (O.R.) and analytics professionals and students. INFORMS provides unique networking and learning opportunities for individual professionals, and organizations of all types and sizes, to better understand and use O.R. and analytics tools and methods to transform strategic visions and achieve better outcomes.
For more information on INFORMS, its publications, membership, or meetings visit http://www.informs.org

Information Systems Research
Vol. 27, No. 4, December 2016, pp. 962–986
ISSN 1047-7047 (print) | ISSN 1526-5536 (online)

https://doi.org/10.1287/isre.2016.0671
© 2016 INFORMS

Why Do Adults Engage in Cyberbullying on Social Media? An Integration of Online Disinhibition and Deindividuation Effects with the Social Structure and Social Learning Model

Paul Benjamin Lowry, Jun Zhang
Faculty of Business and Economics, University of Hong Kong, Pokfulam, Hong Kong
{paul.lowry.phd@gmail.com, junzhangnju@gmail.com}

Chuang Wang
School of Business Administration, South China University of Technology, 510641 Guangzhou, China,
bmchwang@scut.edu.cn

Mikko Siponen
Department of Computer Science and Information Systems, Faculty of Information Technology, University of Jyväskylä,
40014 Jyväskylä, Finland, mikko.t.siponen@jyu.fi

The dramatic increase in social media use has challenged traditional social structures and shifted a great deal of interpersonal communication from the physical world to cyberspace. Much of this social media communication has been positive: Anyone around the world who has access to the Internet has the potential to communicate with and attract a massive global audience. Unfortunately, such ubiquitous communication can be also used for negative purposes such as cyberbullying, which is the focus of this paper. Previous research on cyberbullying, consisting of 135 articles, has improved the understanding of why individuals—mostly adolescents—engage in cyberbullying. However, our study addresses two key gaps in this literature: (1) how the information technology (IT) artifact fosters/inhibits cyberbullying and (2) why people are socialized to engage in cyberbullying. To address these gaps, we propose the social media cyberbullying model (SMCBM), which modifies Akers' [Akers RL (2011) *Social Learning and Social Structure: A General Theory of Crime and Deviance*, 2nd ed. (Transaction Publishers, New Brunswick, NJ)] social structure and social learning model. Because Akers developed his model for crimes in the physical world, we add a rich conceptualization of anonymity composed of five subconstructs as a key social media structural variable in the SMCBM to account for the IT artifact. We tested the SMCBM with 1,003 adults who have engaged in cyberbullying. The empirical findings support the SMCBM. Heavy social media use combined with anonymity facilitates the social learning process of cyberbullying in social media in a way that fosters cyberbullying. Our results indicate new directions for cyberbullying research and implications for anticyberbullying practices.

Keywords: cyberbullying; cyberstalking; cyberharassment; social media; social media cyberbullying model; SMCBM; neutralization; anonymity; disinhibition; deindividuation; differential association; differential reinforcement; definition; imitation; social structure and social learning model; SSSL model; social learning; social learning theory; SLT
History: Rob Fichman, Ram Gopal, Alok Gupta, Sam Ransbotham, Senior Editors; Rob Fichman, Associate Editor. This paper was received on February 23, 2015, and was with the authors 6 months for 4 revisions. Published online in *Articles in Advance* November 18, 2016.

1. Introduction

In 2007, worldwide media reported on the case of Megan, a 13-year-old who was cyberbullied on social media by a "cute boy" named Josh she had met online. The two had an intense online friendship that ended poorly, with Josh branding Megan a "liar and slut." His last message to Megan was "you are a bad person and everybody hates you. Have a s****y rest of your life. The world would be a better place without you" (Pokin 2007). The next day, Megan committed suicide. The startling twist to this story was that Josh was not a teenage boy but an adult female, Lori, who was married with children, had no criminal record, and ran a successful advertising business. She told police she had intended to "mess with Megan" because Megan had fallen out with her daughter, Sarah. It was later discovered that another adult female had helped with the cyberbullying. As this case demonstrates, although cyberbullying is a growing problem with adolescents (Kay 2013), it is also an adult phenomenon that has extended to workplace settings (Acohido 2013). For example, nearly half (46.2%) of trainee doctors have experienced workplace cyberbullying that has negatively influenced their job satisfaction (Farley et al. 2015). In fact, it is estimated that the average online stalker/bully is 41 years old (McFarlane and Bocij (2003).

A recent workplace cyberbullying case is a good illustration of this problem (Pershing Square Law Firm 2013): Ralph Espinoza was mildly disabled and had no fingers on his right hand. In 2006, two of his coworkers anonymously created two personal blogs to publish malicious comments about Espinoza. They referred to him as the "one handed bandit," labeled his right hand "the claw," and offered a reward for photos of his hand. This cyberbullying campaign quickly drew attention from numerous people, including other colleagues and strangers inside and outside the workplace, who also started to cyberbully Espinoza using fictitious (anonymous) names. The harassment continued for over a year and caused Espinoza to take medical leave. Although the cyberbullying extended beyond the workplace, the courts awarded US$820,000 to Espinoza because his employer did not adequately supervise its employees and did not act to thwart the cyberbullying.

Accordingly, widespread concerns about cyberbullying have inspired research on cyberbullying in different disciplines. This literature has included explorations of ethical and moral factors (Tavani and Grodzinsky 2002), gender and age differences (Tokunaga 2010), sociodemographics (Vandebosch and Van Cleemput 2009), and the relationships between online delinquent behavior and psychotic and symptomatic factors (Hinduja and Patchin 2010). Although previous research has improved the understanding of the motivations behind cyberbullying, we highlight two issues that require further study.

First, evidence consistently shows that people are more likely to bully or stalk online than offline (Marcum et al. 2014, Slonje and Smith 2007). Recently, it was even estimated that 3.4 million people over 18 years of age were harassed online in the United States annually (Baum et al. 2009). Although researchers have acknowledged that theories and studies of traditional bullying are not applicable to cyberbullying because of differences between online and offline contexts (Dooley et al. 2009, Hinduja and Patchin 2008, Slonje and Smith 2007), little research has examined exactly what makes the context of cyberbullying different from that of traditional bullying. Four studies that examined this issue highlighted the role of anonymity (Barlett et al. 2014, Udris 2014, Varjas et al. 2010, Wright 2014). Although this is an insightful start, these studies did not present anonymity as it is understood in the theoretical information systems (IS) literature and thus did not explain how and *why* it encourages cyberbullying or what creates anonymity itself. These studies offered only a binary representation of anonymity that focuses on lack of identification (yes/no), even though in an online social context, anonymity is highly perceptual and—aside from lack of identification—includes diffused responsibility, lack of proximity, knowledge of others, and confidence in the system to function (Lowry et al. 2013, Pinsonneault and Heppel 1998).

Second, it has been recognized that cyberbullying in social media can cause more psychosocial and emotional damage than traditional offline physical bullying because of the increased volume, scale, scope, and number of witnesses (Gillespie 2006). Worse still, through social media, cyberbullying can spread with a rapid, broad scale that it is almost unstoppable (Huang and Chou 2010, Li 2008). For example, in the Ralph Espinoza case, the wide exposure to the cyberbullying activities and the extensive interaction with peers exhibiting cyberbullying behaviors on social media demonstrate the potential of social learning and influence to run amok very quickly online. However, we are not exactly sure *why* this social learning and influence occurs. Therefore, a related unexplored issue is to what extent leading social learning and criminology research, such as that involved with social learning theory (SLT) (Akers 2011), can be used to explain cyberbullying, and to what degree such theory must be modified.

Motivated by these issues in cyberbullying research, and by the fact that most studies focus on adolescents (adult cyberbullying is overlooked in research (Nycyk 2015) and is generally ignored in management practice, even though much occurs at work or among coworkers (Baum et al. 2009)), we propose a new model to explain adult cyberbullying that accounts for the social media artifact of perceived anonymity in a social learning context. Our model, the social media cyberbullying model (SMCBM), builds upon Akers' (2011) seminal work on criminology and deviance. Our study aims to explain the pervasiveness and high transmissibility of adult cyberbullying by adopting the perspective of SLT, which posits that criminal behaviors are learned through association with deviant others (Akers 2011). We thus also examine the extent to which the social learning components (including differential association, reinforcement, and definition) that are relevant to traditional (noncyber) deviance and crime are also relevant to cyberbullying (e.g., Akers 2011), and if so, how any of these are influenced by perceived anonymity and the use of social media. We tested the SMCBM with 1,003 adult social media users who had a range of experiences with different types of cyberbullying. The results support the SMCBM and lay a foundation for compelling future cyberbullying research.

2. Background on Cyberbullying

2.1. Defining Cyberbullying

The literature does not clearly distinguish between cyberbullying, cyberstalking, and cyberharassment. *Cyberbullying* generally refers to deliberate and hostile behavior intended to harm people using the Internet by leveraging the imbalance of power between bullies and victims (Limber 2012, Smith et al. 2008). Notably, cyberbullying can involve stalking behaviors—such as sending threatening and harassing emails or messages and passing on rumors—as well as harassment, flaming, and denigration (Li 2006). *Cyberharassment* can be defined as repeated or one-off malicious Internet behaviors that are unsolicited but noticed by victims, which are intended to upset, disturb, or threaten other people (Piotrowski 2012, Workman 2010). *Cyberstalking* generally refers to a series of repeated intrusive behaviors performed via the Internet, such as gathering private information or direct communication, that are intended to convey implicit and explicit threats and thus induce fear in online victims (Bocij 2004, Meloy 2001, Robert and Doyle 2003). "Cyberstalking is also known by other names such as online harassment, online abuse or cyberharassment" (Philips and Morrissey 2004, p. 67). However, unlike cyberbullying and cyberharassment, cyberstalking might involve following a former lover online but not involve harassing behaviors (i.e., victims do not always know they are victims).

In reviewing these definitions, we consider cyberstalking and cyberharassment to be specialized forms of cyberbullying. Moreover, we argue that cyberbullying is a more appropriate term for the current study because cyberstalking generally involves repeated behaviors (Meloy 2001), whereas our scope includes one-off harassing behaviors. Moreover, cyberbullying typically involves aggressive behavior and an imbalance of power (Sourander et al. 2010). Such deliberation and power imbalance causes more psychosocial and emotional damage than traditional offline physical bullying (Gillespie 2006). Thus, given our context, when we refer to *cyberbullying*, we refer to social harassment on social media, whether it takes the form of stalking, bullying, or harassment. Our definition necessarily excludes other online deviant behaviors with a weaker social media and interpersonal orientation, such as Internet addiction, pornography addiction, computer abuse, and online scams.

2.2. Gaps in the Cyberbullying Literature

Studying adult cyberbullying is challenging because most of the research involves juveniles, and the nascent literature has not yet developed a cohesive approach to studying cyberbullying. However, this broader cyberbullying literature is arguably the best starting point for building a theoretical model to better understand adult cyberbullying. We thus performed a review of the related literature (135 articles), as detailed in Online Appendix A (available as supplemental material at https://doi.org/10.1287/isre.2016.0671). In this section, we summarize how this review informed our theory building. Of the 135 articles, fewer than half provided empirical evidence, and most of those that did were atheoretical and focused on juvenile offenders. A large portion of these studies have nonetheless appeared in high-quality and high-impact-factor journals, as noted in Online Appendix A.

In the cyberbullying articles that were theory driven and supported by empirical evidence, the most frequently used theories were from psychology and criminology, including general strain theory, SLT, social cognitive theory, social norms theory, social dominance theory, and social ecological theory. However, these theories are either *macrolevel* (environment level) theories that explain how cyberbullying can be directly influenced by the general environment or *microlevel* (individual level) theories that investigate the cognitive processes of individuals when they are involved in cyberbullying. Thus far, the cyberbullying literature has not established a theoretical integration of the macro- and microperspectives, which has been achieved elsewhere in the deviance literature of Akers (2011). Thus, cyberbullying research currently lacks a cohesive theoretical approach to unifying inconsistent results.

Moreover, simply adopting models that were derived from offline/physical contexts is unlikely to result in accurate explanations of the unique social media context of cyberbullying. Although the cyberbullying literature is replete with claims that the nature of cyberbullying is different from that of offline bullying, most of these studies have glossed over the central issue: the role of information technology (IT) or social media artifacts themselves in promoting cyberbullying. Most of the reviewed studies have inferred or acknowledged in passing that such artifacts are factors, but have rarely explained these factors theoretically. For example, Raskauskas and Stoltz (2007, p. 566) made two brief mentions of the "anonymity of electronics," with no further explanation, measurement, or modeling. Interestingly, although they cited Ybarra (2004) as support for electronic anonymity, Ybarra's (2004) study did not mention anonymity. Even the most recent cyberbullying study, which is forthcoming in a top journal, only mentioned anonymity in passing (Barlett et al. 2016). This literature is replete with this kind of insubstantial treatment of and vague assumptions regarding anonymity. However, this point is not meant to condemn the current research, because it has been conducted primarily by psychologists and sociologists, whose focus is not on social media artifacts and how they might foster anonymity. This is where IS research can contribute.

To date, only four studies have dealt with IT artifact issues (doing so as a secondary consideration), and three of these offered only a binary representation of anonymity, which focused on lack of identification (yes/no) (Barlett et al. 2014, Varjas et al. 2010, Wright 2014). Another study inferred anonymity but focused more on the role of the disinhibition/disassociation created by online interactions (Udris 2014). Thus, the qualitative account by Varjas et al. (2010) of 20 high schoolers stands out as particularly insightful because it addresses both anonymity and disinhibition.

The initial work on the cyberbullying IT artifact is a good start, but it is not a complete picture of anonymity or disinhibition in cyberbullying, and it omits explanations of causal mechanisms, which are crucial to theory building. Again, IS researchers have discovered that in an online social context, anonymity is highly perceptual and involves not just a lack of identification but also diffused responsibility, lack of proximity, knowledge of others, and confidence in the system's functionality (Lowry et al. 2013, Pinsonneault and Heppel 1998). Outside of cyberbullying, these two studies and others have pinpointed the important underlying mechanisms of disinhibition (e.g., Suler 2004) and deindividuation (e.g., Silke 2003) in changing people's online behaviors.

3. Theory: The SSSL Model in Cyberbullying Contexts

Given the opportunities revealed from the literature, we first propose a theoretical model that includes both macro and micro components related to social learning. We do so by adopting, for the first time in cyberbullying research, a criminology theory that was designed for macro and micro components. Our model is a contextualized version of Akers' (2011) social structure and social learning (SSSL) model of crime and deviance. The SSSL model builds on the core social learning (i.e., micro) components of SLT, which Akers himself developed. For the macro components, the SSSL model adds environmental social structure and sociodemographic factors that drive the model.

Accordingly, before formally proposing our model, we present its theoretical foundation. We first explain the micro factors derived from SLT. We then explain the macro factors derived from the SSSL model. Next, we propose our model, which is a unique contextualization of the SSSL model that accounts for social media artifacts that foster anonymity and related disinhibition and deindividuation. We posit that these factors change the nature of social learning such that cyberbullying is fostered.

3.1. An Overview of SLT and Its Response to Sutherland's (1947) Theory of Differential Association

Akers' early education and career took place during an era when Sutherland's (1947) theory of differential association was widely used to explain crime (Akers 2011) but was beginning to be criticized. Sutherland (1947) suggested that deviant behavior is not genetically inherited or predetermined, nor is it learned through media, news, or movies (a point we later challenge with social media, which allows people unprecedented association opportunities). Sutherland maintained that in American society, individuals associate personally with both law-abiding people and criminals. Whether a person becomes a deviant or a law-abiding citizen depends on the extent to which the individual has been exposed to criminal values (associated differently) versus law-abiding values. Ultimately, criminal behavior is socially learned in the same way as law-abiding behavior (Sutherland 1947). A key critique of Sutherland's differential association is that he did not specify the precise underlying learning mechanisms (Akers 2011), except for noting that learning is more than simple imitation and that it can include gestures and verbal communication (Sellers and Winfree 1990, p. 23). Besides lacking accurate specification of the learning process, Sutherland also did not address the order in which the learning process takes place (Cressey 1960, p. 54).

Burgess and Akers (1966) addressed these criticisms by positing that Skinner's (1953) psychological behaviorism could supply relevant information by specifying the underlying learning mechanisms that Sutherland's theory lacked. This was not the only modification that Akers (2011) proposed. Besides modifying Sutherland's (1947) definitions, Akers et al. (1979) modified the underlying learning mechanism using Bandura's (1977) cognitive SLT and introduced the concepts of imitation and reinforcement into his theory of social learning (Akers 1973, Sellers and Winfree 1990). The resulting theory was called the SLT of crime (Akers et al. 1979), which included "differential association, differential reinforcement, imitation, and definitions" (Akers 2011, p. 50). Although each element can be expressed in the form of an individual hypothesis, an underlying assumption of SLT is that these elements are considered as a whole (Akers 2011). This means that when all of the elements lean more toward deviant behaviors, the probability of deviant behaviors increases (Akers 2011, p. 48).

3.2. The Core Components of SLT

3.2.1. Differential Association. In contrast with earlier literature (for example, Cohen 1955 proposed the subculture theory of crime, according to which crime and criminal attitudes are formed within gangs and criminal subcultures), associations in SLT do not refer to particular gang or criminal subcultures, although these can also be differential associations. For Sutherland (1947), and even more so for SLT, associations refer to any social interactions. Consequently, *differential association* is the process by which individuals directly and indirectly interact and identify with others to learn deviant or acceptable behaviors (Akers et al. 1979). For SLT, the relevant social groups can change during an individual's development (Akers 2011). In relation to cyberbullying, differential association means that cyberbullies in the making associate with different social groups (i.e., ones with cyberbullies in them) than conforming people (i.e., noncyberbullies).

SLT emphasizes that differential association results in interactional peer influence but not peer pressure, which plays only a marginal role in deviant behavior (Akers 2011, p. 63). When individuals are associated with people who perform certain behaviors, they are provided with a social environment "in which exposure to definitions, imitation of models, and social reinforcement for use of or abstinence from any particular substance take place" (Akers et al. 1979, p. 638). Thus, deviant acts are partially learned from deviants. Likewise, nondeviant acts are learned from nondeviants (Akers 2011). Recent research has suggested that in a social media context, differential associations can include online friends, influential online personalities (e.g., bloggers and celebrities), and even anonymous virtual group members, in addition to offline intimate personal groups (Hawdon 2012, Pauwels and Schils 2016). We leverage these social media-related insights in our theoretical model.

3.2.2. Differential Reinforcement. *Differential reinforcement* deals with the frequency, amount, and probability of rewards and punishments associated with a behavior, whether experienced personally or anticipated by observing the consequences to others. Akers (1998) points out that differential reinforcement is considered "the core behavior-shaping mechanism" (Tittle et al. 2012, p. 864) of SLT, because all of the cognitive and noncognitive elements of social learning (i.e., *definitions*, *imitation*) are first shaped largely by the reinforcement process. In general, if rewards and positive consequences are observed, the behavior will be reinforced over time; conversely, if punishments and negative outcomes are observed, the behavior will be thwarted over time.

There are four reinforcement mechanisms that can either strengthen or weaken a behavior (Akers 2011): (1) *positive reinforcement* (providing rewards), (2) *negative reinforcement* (removal of punishments), (3) *positive punishment* (providing punishment), and (4) *negative punishment* (removal of rewards). Although there are similarities between these concepts and their counterparts in deterrence theory and rational choice theory (RCT), they should not be conflated.

Differential reinforcements may seem similar to deterrence and rational choice theories of crime. For example, deterrence theory includes punishment, and the RCT of crime entails sanctions and rewards (Akers 1990). Deterrence theory also features specific deterrence, which is self-learned consequences, and general deterrence, which is the observed experience of others being punished (Gibbs 1975). Thus, deterrence theory implicitly entails learning, but unlike SLT, deterrence theory does not outline specific learning mechanisms beyond specific and general deterrence (Gibbs 1975). Also, deterrence theory does not highlight the roles of associations, definitions, or balance probability (e.g., rewards and costs; Gibbs 1975). The RCT of crime, especially Becker's (1968) early version, involves rational calculations intended to maximize benefits, and it is therefore an economic analysis of crime. SLT does not explain crimes in terms of rational cost–benefit calculations aimed at maximizing benefits, but rather as actions learned through associations with criminals.

3.2.3. Imitation. The imitation construct was later added to SLT by Akers et al. (1979), following Bandura's (1977) theorizing.[1] *Imitation* takes place when one observes behaviors and behavioral consequences and then decides to do the same (Akers 2011). Pondering the consequences of a behavior links imitation to reinforcement. It is crucial to SLT that when people are exposed more to deviant role models than to nondeviant role models, they are more likely to imitate the deviant role models (Sellers and Winfree 1990). The learning mechanisms, which for SLT includes imitation and observational learning, explain not only how people become deviants but also the maintenance and desistance of deviant behavior (Akers 2011). However, SLT posits that imitation is "more important in the initial acquisition and performance of novel behavior than in the maintenance or cessation of behavioral patterns once established" (Akers and Sellers 2004, p. 89). Akers et al. (1979) suggest that "after the initial use, imitation becomes less important" (Akers et al. 1979, p. 638) in predicting sustained behavior. They found that imitation variables explain "almost none of the variance" (for about only 0.1% of various kinds of abuse behavior) in predicting longitudinal deviant behaviors (Akers et al. 1979, p. 651). Thus, we do not model or measure it and instead assume it to be a causal mechanism of the social learning process.

[1] Adding imitation and downplaying Skinnerian operant conditioning also moved the SLT from the "Skinnerian behaviorism" version of Burgess and Akers (1966) toward cognitive learning theories (Akers 2011).

3.2.4. Definitions. In SLT, *definitions* "are orientations, rationalizations, definitions of the situation, and other evaluative and moral attitudes that define the commission of an act as right or wrong, good or bad, desirable or undesirable, justified or unjustified" (Akers and Sellers 2004, p. 86). Notably, definitions arise from the vicarious experience of differential reinforcement and the direct experience of imitating others. For SLT, because definitions can strengthen deviant behavior, they play a key role in explaining deviant behavior. Akers (2011) distinguished among three types of definitions: positive, negative, and neutralizing. Positive definitions result in the approval or acceptance of deviant behavior, negative ones result in the disapproval of such behavior, and neutralizations result in behavioral justification, which at a minimum is a form of positive, temporary approval. In this way, Akers (2011) links neutralizations, originally put forward by Sykes and Matza (1957), to definitions. Akers (2011) views neutralization as an extension of differential association theory in the sense that neutralizations are learned from deviant peers. Using neutralization techniques, deviants accept deviant acts as "'all right' under certain conditions" that are seen as "exceptional" (Akers 2011, p. 36). Thus, deviants use neutralization techniques to characterize a given set of conditions as exceptional, which in turn makes an act that in other circumstances would be morally unjustifiable feel acceptable.

3.3. The SSSL Model: Integrating Social Structures with SLT

The SSSL model is an extension of SLT that adds macro factors to the micro factors of SLT.[2] As a framework for cross-level theory integration, the SSSL model makes it possible to combine macrolevel social structure theories with microlevel social learning variables to explain deviant behaviors. The motivation for considering the influence of social structure variables in SLT is that social structure determines the "general culture and structure of society and the particular communities, groups, and other contexts of social interaction" (Lee et al. 2004, p. 17) that influence social learning mechanisms, including the people with whom one is associated, reinforcement stimuli in the learning environment, and group norms regarding what is approved and disapproved. Online Appendix B summarizes our literature review of the SSSL model-based studies on which we build. Only two of these (Holt et al. 2010, Morris and Higgins 2010) have investigated a form of cyberdeviance using the SSSL model. Neither Holt et al. (2010) nor Morris and Higgins (2010) studied how social media artifacts influence social learning.

In the SSSL model, *social structure* "can be conceptualized as an arrangement of sets and schedules of reinforcement contingencies and other social behavioral variables" (Lee et al. 2004, p. 17) that create a deviance-producing or deviance-preventing environment that shapes an individual's behavior through the social learning process (Verrill 2005). In the SSSL model, Akers (2011) distinguishes four categories of social structural variables that can be used to predict social learning, as shown in Figure 1.

The four categories are (1) structural crime correlates, which include geographical, societal, cultural, social, and community differences; (2) sociodemographic and socioeconomic crime correlates, which deal with one's location in the social structure (e.g., age, gender, income, employment, class, and religion); (3) theoretically defined structural causes, such as those involving social disorganization (e.g., class conflict, oppression, and racism); and (4) differential social locations of primary and secondary reference groups (e.g., family, peers, church, school, and work). The effects of structural variables on crime mean that a person's race or place of residence do not directly cause crime. Rather, structural variables explain why people of certain ages or races may associate with certain reference groups, from whom they learn definitions, crime techniques, and differential reinforcements of criminal behavior.

3.4. Proposing the SMCBM Based on the SSSL Model and SLT

Here, we present an overview of how we contextualize the SSSL model for cyberbullying, which results in the SMCBM. Figure 2 outlines this proposed theoretical model. Table 1 summarizes how we map the key social learning constructs to constructs that are more closely contextualized to cyberbullying. As follows, we explain how cyberbullying maps to the SSSL model and SLT. In the hypothesis section, we then return to the Ralph Espinoza case and discuss it using these principles.

First, although there is no strict order in which the social structure elements must be applied, we posit that moving from offline social interactions to interacting through social media can result in a meaningful shift in a person's social environment. The social group one affiliates with offline is replaced by the group of people one observes or interacts with on social media (i.e., structural correlates/social organization (the first SSSL model category) and

[2] The SSSL model encompasses SLT because it uses social structure variables as predictors, SLT constructs as mediators, and deviance as the dependent variable (Akers 2011). The influence for this integration came, once again, from Sutherland (1947, p. 8), who had already described that social structures "determine" social associations. Cressey (1960) had also asserted that crimes in the United States vary according to social structural indicators such as class, gender, and race. Akers (2011, p. 320) built on this notion with the SSSL model to suggest that social structures do not have a direct effect on deviant behavior, but that these structures affect social learning elements, which then drive deviance. This also explains the correlation between social structure and crime rate (Akers 2011).

Figure 1 An Overview of Akers' (2011) SSSL Model, Which Extends SLT

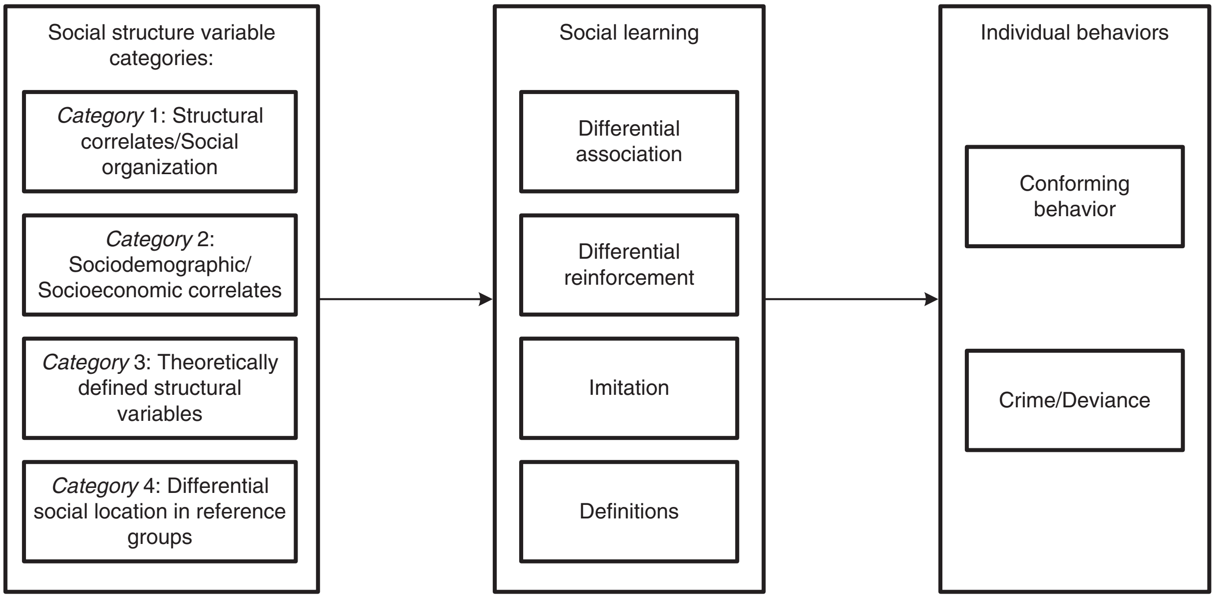
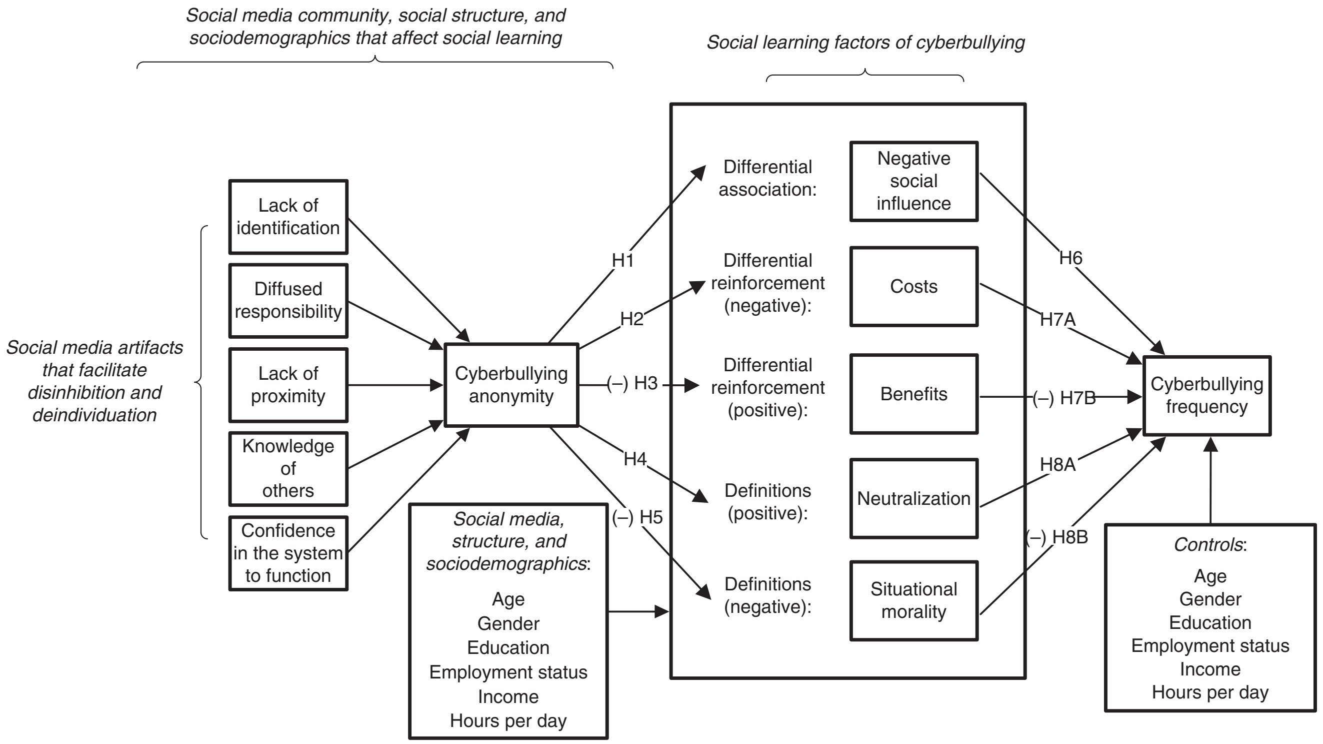

Social structure variable categories:
Category 1: Structural correlates/Social organization
Category 2: Sociodemographic/ Socioeconomic correlates
Category 3: Theoretically defined structural variables
Category 4: Differential social location in reference groups
Social learning
Differential association
Differential reinforcement
Imitation
Definitions
Individual behaviors
Conforming behavior
Crime/Deviance

Figure 2 The Proposed Theoretical Model: The Social Media Cyberbullying Model


Social media community, social structure, and sociodemographics that affect social learning
Social learning factors of cyberbullying
Social media artifacts that facilitate disinhibition and deindividuation
Lack of identification
Diffused responsibility
Lack of proximity
Knowledge of others
Confidence in the system to function
Cyberbullying anonymity
H1
H2
(–) H3
H4
(–) H5
Differential association:
Differential reinforcement (negative):
Differential reinforcement (positive):
Definitions (positive):
Definitions (negative):
Negative social influence
Costs
Benefits
Neutralization
Situational morality
H6
H7A
(–) H7B
H8A
(–) H8B
Cyberbullying frequency
Social media, structure, and sociodemographics:
Age
Gender
Education
Employment status
Income
Hours per day
Controls:
Age
Gender
Education
Employment status
Income
Hours per day

differential social location in reference groups (the fourth SSSL model category)). Thus, whether lurking and observing a heated Discuss debate on rival sports teams or actively engaging in discussions about politics on Facebook, a person takes up a virtual affiliation with a subcommunity and starts to internalize its rules of engagement and norms regarding cyberbullying. Characteristics of these social media subsocieties—such as culture, social cohesion, social stability, surveillance, and informal control—can also differ across different forms of social media. For example, some Reddit communities might have strict moderators (moderators are a common feature in this tool) who block people for cyberbullying, whereas others might be known for unmoderated bullying behavior.

Table 1 Mapping of Key Social Learning Factors to This Research

Social learning concept	Definition of construct from SLT	Constructs used in our research model
Differential association	The process by which individuals directly and indirectly interact and identify with others who already engage in deviance to learn deviance, through the norms and frequency of these behaviors	We use *cyberbullying negative social influence* (*norms* and *frequency*) to reflect the extent to which individuals are exposed to the norms and cyberbullying of people who are socially important references (e.g., friends, family, colleagues, and people they follow online).
Differential reinforcement (including imitation)	The frequency, amount, and probability of rewards (i.e., negative reinforcement, encouraging deviance) and costs/punishment (i.e., positive reinforcement, blunting deviance) associated with deviant behaviors (both through one's own experiences and through vicarious experiences of observing others through differential association); this subsumes the potential imitation process of social learning[a]	To represent negative differential reinforcement, we use *cyberbullying costs*, which represents a person's perceptions of any potential intrinsic or extrinsic losses that could occur from a cyberbullying act. To represent positive differential reinforcement, we use *cyberbullying benefits*, which represents a person's perception of the potential intrinsic or extrinsic gains that could occur from a cyberbullying act.
Formation of definitions	Whether a deviant behavior is perceived as good or bad based on learned attitudes, beliefs, morality, and neutralization; the neutralizing definition is whether the deviant behavior can be justified as good	We use *cyberbullying situational morality* as a positive definition to reflect the extent to which a person believes a given form of cyberbullying to be unethical. We use *cyberbullying neutralization* as a negative definition to represent the degree to which a person suspends their offline moral judgment and instead rationalizes a given form of cyberbullying as acceptable.

[a] Definitions and imitation were added to SLT by Akers et al. (1979) as extensions of differential reinforcement. In this process of reinforcement through vicarious experience, if individuals perceive in others' experiences high benefits and low costs, they are more likely to imitate the behavior. Although imitation plays an important role in initiating deviant behavior and is thus a potential fourth key SLT factor, we removed it because it is not useful in predicting sustained behavior (Akers et al. 1979).

Second, the scale and scope of cyberbullying allows people, through social media, to affiliate and interact with more communities than is possible through other means. We describe this as increased "social media reach." Today, unlike in any other time in history, a person in Des Moines, Iowa, can communicate with and befriend someone—whom they have never met in person—in Tanzania, and have similar relationships with hundreds of others. Unfortunately, the same is true for bullying. Social media allows different kinds of people (e.g., with different sociodemographic/socioeconomic backgrounds) to affiliate with the same social communities (i.e., social structure categories 2 and 3).

For cyberbullying, the greater social media reach provided means that people can observe a greater variety of bullying, differing norms regarding cyberbullying, and a greater variety of bullies (e.g., children; working adults; parolees; celebrities; politicians; felons; sex offenders; cult members; retirees; veterans; lesbian, gay, bisexual, and transgender advocates; terrorists; and "shut-ins"). We use standard elements of social structure category 2 (i.e., structural crime correlates) using basic demographics that are typically used as social learning correlates (e.g., gender, age, education, income, employment), but we also add a crucial factor for social media that should drive one's exposure to negative social influence (NSI): hours of social media use per day.

Third, we posit that the social media artifact itself changes the social structure; that is, social media strengthens the perception of anonymity, which fosters the underlying causal mechanisms of online disinhibition and deindividuation that change social learning and encourage cyberbullying. When people feel anonymous online and are considering cyberbullying, their increased disinhibition and deindividuation will change their differential reinforcement to downplay perception of risk and exaggerate perception of reward. Likewise, their definitions will be skewed such that negative definitions (e.g., neutralization) will increase and positive definitions (e.g., situational morality) will increase. These will then foster cyberbullying. Importantly, all of these social learning factors are reciprocal and self-reinforcing over time, as emphasized in the literature, even though they are rarely measured as such (Akers 2011). Next, we explain the causal mechanisms of perceived anonymity on social media.

3.5. How Social Media Fosters Perceived Anonymity

We argue that perceived anonymity plays a role in traditional crimes, even though criminological theories (e.g., SLT, deterrence theory, and RCT) may not specifically or directly theorize this role. (For example, a robber may use a mask in an attempt to avoid identification.) Although anonymity is not formally identified by criminological theories, several studies of criminology and deviance highlight the role of perceived anonymity in fostering deviant outcomes. For example, urban settings with a higher population density and population mobility help to foster a sense of anonymity that enables crime and deviance (Clear et al. 2003, Crutchfield 1989, Crutchfield et al. 1982).

Never mind that in urban environments, perpetrators are more likely to be caught on camera than in nonurban environments—perceptions are what matter. For instance, Clear et al. (2003) and Warner and Pierce (1993) suggest that environments perceived as anonymous as a result of residential mobility reduce people's sense of commitment, surveillance, and informal social control, which further weakens social stability (Crutchfield et al. 1982). Similarly, according to Trumbull (1989), a more anonymous environment created by overcrowding (high population density) increases criminal opportunities. Danzinger (1976, p. 292) also points out that "anonymity makes identification of criminal suspects more difficult;" thus, crime rates in large cities tend to be higher because of the reduced apprehension of perpetrators. Jackson (1991, p. 384) argues that anonymity decreases social cohesion and restrains law enforcement, which influences "the ease of crime commission." Thus, anonymity serves as a macrolevel predictor of general deviance in the physical world, and its role is stronger online.

However, perceived anonymity is much more complex than mere lack of identification. The five related subconstructs of perceived anonymity established by Pinsonneault and Heppel (1998) are foundational to our explanation of how social media artifacts change the social structure that influences social learning: lack of identification, diffused responsibility, lack of proximity, lack of knowledge of others, and confidence in the system's functionality. Building on Pinsonneault and Heppel (1998) and Lowry et al. (2013), we define these subconstructs as follows: *lack of identification* is the degree to which potential cyberbullies believe their personal identities will not be revealed by the social media system; *diffused responsibility* is the degree to which potential cyberbullies believe they will not be held accountable for their cyberbullying on social media; *lack of proximity* is the extent to which potential cyberbullies believe others are not physically close enough to their computer to observe their cyberbullying; *lack of knowledge of others* is the degree to which potential cyberbullies believe others in the social media system do not know them well enough to recognize them; and *confidence in the system to function* is the degree to which potential cyberbullies have confidence that the social media system will not malfunction, involve secret monitoring, or have "back doors" that will reveal their identity against their wishes. Given these definitions, it is clear that the meaning of anonymity is richer in a social context (Lowry et al. 2013) in which "anonymity can only significantly affect disinhibition, and other behaviors in general, when social evaluation is an important source of inhibition" (Pinsonneault and Heppel 1998, p. 97). We argue that perceived anonymity's role in cyberbullying is multidimensional and subjective.

Several key factors explain why the five factors of perceived anonymity are altered in social media social structures and why they are highly subjective. First, several technical features of social media allow for increased anonymity, such as using pseudonyms, throwaway accounts, and false identities (i.e., lack of identification). Second, many sophisticated tools can be used outside of social media (e.g., browser extensions) that can further hide identity from social media providers (i.e., lack of identification and confidence in the system). Third, people are more likely to harass or bully people they do not know (Ybarra and Mitchell 2004; i.e., knowledge of others and lack of proximity). Fourth, social media introduces dramatic shifts in scope and scale. Users can target thousands of people, engage in more frequent and more intense interactions, and reach people who are unreachable offline (Mangolda and Faulds 2009; i.e., diffused responsibility and knowledge of others). Fifth, prosecuting cyberbullies requires law enforcement authorities to obtain Internet protocol (IP) addresses and other information from Internet service providers, which often are located in different countries or jurisdictions only governable by national law enforcement (i.e., diffused responsibility and confidence in the system). This means that cyberbullying is difficult to prosecute even when it involves a crime (e.g., a direct threat) and that people are less likely to witness the arrests and prosecution of cyberbullies.

3.6. How Cyberbullying Anonymity Fosters Disinhibition and Deindividuation and Changes Social Structure and Social Learning

We now explain that perceived anonymity facilitates the underlying causal mechanisms of disinhibition and deindividuation, and it is these factors that desensitize people such that their social learning is altered to increase their willingness to engage in cyberbullying. Just as alcohol may disinhibit some people and consequently give them the courage (or stupidity) to pick a fight with a member of a biker gang at a bar, anonymity's disinhibition and deindividuation mechanisms foster acts of online deviance in which people would not normally engage.

The relationship between criminal behavior and the anonymity of cyberspace has been found to be significant in two empirical studies (Baggili and Rogers 2009, Barlett and Gentile 2012), but it has not been clearly explained. The theory of online disinhibition—which posits that several macrolevel online characteristics are related to the high rate of online crime/deviance (Suler 2004)—offers an explanation for the prevalence of online deviance. Li (2007, p. 1780) likewise argues that anonymous computer-mediated communication "not only fosters playful disinhibition but reduces social accountability," leading to more engagement in aggressive acts. Consistent with this claim, Delmonico and Griffin (2008, p. 461) suggest that online disinhibition explains "why the Internet is an ideal venue for problematic sexual behavior." Lapidot-Lefler and Barak (2012, p. 434) have also used online disinhibition to explain flaming behavior and suggest that the disproportionately high occurrence of deviant behaviors such as "violence, incitement, flaming, and verbal attacks" on social media should be attributed to online disinhibition. Thus, we argue that because of the distinct nature of social media, disinhibition effects will influence the social psychological process of individuals committing cyberbullying. Specifically, *online disinhibition* occurs when individuals feel free to perform behaviors in cyberspace that they feel inhibited from performing offline (Lowry et al. 2013, Suler 2004).

Importantly, in describing the disinhibition effect, Suler (2004) regards anonymity as the principal factor of increased disinhibition online, which in turn leads to cyberdeviance. For concision, we too focus primarily on anonymity; it allows more straightforward conceptualization and measurement. According to Suler (2004), the disinhibition effect occurs because a high degree of anonymity enables people to easily separate their online actions from their offline identities and "avert responsibility for those behaviors, almost as if superego restrictions and moral cognitive processes have been temporarily suspended from the online psyche" (Suler 2004, p. 322). Such disinhibition has been predicted to exert significant influence over cyberbullying (Hinduja and Patchin 2008) and cyberstalking (Bocij and McFarlane 2003), but our study is the first to explain and test this relationship.

The second causal mechanism fostered by anonymity is *deindividuation*, which is "the loss of one's sense of individuality and personal responsibility" (Valkenburg and Peter 2011, p. 122). It has been shown that anonymity (either in online or offline settings) is one of the major causes of deindividuation (Silke 2003). Anonymous conditions facilitate deindividuation by causing a loss of self-awareness (Silke 2003). The social identity model of deindividuation (Reicher et al. 1995) also proposes that "anonymity promotes a shift in the kind of self-awareness from the personal to the group" (Lea et al. 2001, p. 527; in this model, the process is also called depersonalization). The "sense of responsibility for actions online" (Cooper and Blumenfeld 2012, p. 159) will be inhibited, and individuals may convince themselves that they are not responsible for their online deviant behaviors (Freestone and Mitchell 2004, Harris and Dumas 2009). In addition, depersonalization caused by anonymity magnifies the influence of group norms and thereby makes it easier for individuals to learn negative definitions from deviant peers (DeHue et al. 2008).

4. Operational Model and Hypotheses

The hypotheses, depicted in Figure 2, closely follow our theoretical review that created the SMCBM, which is a modification of the SSSL to fit the cyberbullying context. Here, we start with predictions of how the IT artifact of cyberbullying anonymity changes the influence of the social learning constructs. We then explain how these influence cyberbullying frequency. We refer back to the Ralph Espinoza case as an illustration of these relationships and of how social learning influences cyberbullying.

4.1. How the IT Artifact of Perceived Anonymity Can Change Social Learning Outcomes

4.1.1. How Cyberbullying Anonymity Influences Differential Association. Again, in our context, *differential association* is the process by which individuals directly and indirectly interact and identify with others who engage in deviant behaviors to learn such behaviors. Consequently, our surrogate for this construct is negative social influence. We argue that perceived anonymity online encourages more association with those who engage in deviant behaviors. In the Ralph Espinoza case, anonymity allowed more coworkers to join. Worse, it allowed unknown people outside of work to observe and join the negative social spectacle.

We posit that anonymity fosters this problem for a couple of reasons: Most importantly, online anonymity allows one to associate with people who engage in deviant behaviors with whom one would not normally associate offline because of social restraint and potential embarrassment, as well as lack of access/reach. According to Neal (2010), people with relatively good social status are less willing to be associated with aggressive peers in a nonanonymous setting, because association with deviant peers can damage their social position. However, such restraint does not exist if aggressive behaviors are conducted anonymously. In the Ralph Espinoza case, people from outside work anonymously joined the fray in large numbers; this would be highly unrealistic in the physical world. Recall that a key causal mechanism of anonymity is behavioral disinhibition (Lowry et al. 2013, Suler 2004). Such inhibition should also extend to association; that is, it should be much easier and less risky to associate with social deviants anonymously online (e.g., associating with highly profane, angry, criminal, or racist people) than to do so offline. For example, it is much less socially risky for most people to visit a neo-Nazi Subreddit anonymously than to attend a neo-Nazi recruitment meeting. Notably, the more one affiliates with deviant groups or people, the more negative social influence will be experienced, which we explain next.

Both the SSSL model and the SLT posit that deviant behaviors are learned from behavioral models that emerge during social interaction. Differential association attempts to capture the extent to which individuals are exposed to deviant behavior through their associations with others. In the physical world, SSSL indicates that the association would be a physical association with criminals. In our context, we posit that instead the association is virtual and involves observing cyberbullying on social media. This negative exposure is called NSI. Such negative social influence is associated with traditional crimes (Kahan 1997). In our context, NSI can be expressed from the SLT literature (Akers et al. 1989) as a *subjective norm* (the degree to which one perceives important referent others approve/disapprove of specific behaviors; Ajzen 1991) and *frequency* (how often behavior is observed) as the perception that comes into play when individuals learn to perform cyberbullying from others online by virtue of SLT phenomena, such as differential reinforcement and definitions. This is shown in the Ralph Espinoza case: the more people got involved, the less people spoke out, and the longer it went on, the worse the cyberbullying became.

Moreover, such anonymity allows for "lurking" behaviors in which one can observe offensive behaviors online committed by others without any public or social responsibility to speak out against them. In the Ralph Espinoza case, no one—including management—spoke out against what was happening. Through social media, one can witness offensive cyberbullying, but no one has to know that one was a witness. We argue that this can foster an online version of the *bystander effect*. This effect has been documented to occur in physical environments in which bystanders do not offer any help to a victim, and it tends to increase the more people are present because of a sense of diffused responsibility, ambiguity, and cohesiveness (Darley and Latané 1968). Preliminary research indicates that such effects could occur online in chat rooms as people see more users being added to a room (Markey 2000). Similarly, anonymity should make such effects stronger for cyberbullying on large social media platforms, especially because of the previous literature we noted showing a connection between anonymity and deindividuation, which helps foster a loss of one's sense of individual responsibility (Freestone and Mitchell 2004, Harris and Dumas 2009, Valkenburg and Peter 2011), fostering NSI. Thus:

Hypothesis 1 (H1). *An increase in anonymity is associated with increased cyberbullying NSI.*

4.1.2. How Cyberbullying Anonymity Influences Differential Reinforcement. Again, *differential reinforcement* deals with the frequency, amount, and probability of rewards and punishments associated with a behavior, whether experienced personally or anticipated by observing the consequences to others (Akers 1990). Thus, the more an outcome is perceived on the basis of social learning as negative (e.g., as a *cost*), the more likely it discourages those behaviors (Akers 1990). We contend that perceptions of anonymity disrupt normal social structures such that a large volume of bullying is witnessed without negative consequences, and normal calculations of cost–benefit are skewed such that benefits are artificially inflated and costs are not fully manifested or perceived. The Ralph Espinoza case went on for a year and a half without any punishments or chastisement from management; meanwhile, those who participated had the rewards of increased social bonding, power, and entertainment from otherwise dull work. Hence, their differential reinforcement was skewed by the anonymity provided by social media. In the context of nonanonymous abuse, such behavior likely never would have carried on for so long, and it could not have involved as many people.

Because of a lack of anonymity in the physical world, people have a higher chance of witnessing bullies getting caught and receiving sanctions, which may include anything from negative peer reactions to work suspensions to legal consequences. Conversely, social media that is perceived as anonymous is often loaded with rude expressions, name-calling, and insulting language. Because of anonymity, the resulting punishments and social disapproval tend to be weaker and harder to enforce. According to SSSL, via differential reinforcement over time, this explains why users can perceive the costs of cyberbullying as low.[3] The online disinhibition effect can further explain calculations of reduced costs because anonymity enables people to "avert responsibility for those behaviors" (Suler 2004, p. 322). Moreover, the criminology literature shows that anonymity weakens informal social controls (Clear et al. 2003), which suggests that informal costs are reduced online as well.[4] This shift in the social environment through increased anonymity skews the cyberbullying social learning reinforcement process toward diminishing costs. Thus:

Hypothesis 2 (H2). *An increase in anonymity is associated with decreased cyberbullying costs.*

[3] Other studies have also reported that perceived anonymity can make cyberbullies believe that potential sanctions are low: "Anonymity and confidentiality on the Internet provides [sic] a degree of protection for cyber bullies" (Topcu et al. 2013, p. 149); moreover, "anonymity also implies the absence of consequences, because the aggressors frequently cannot be identified" (Calvete et al. 2010, p. 1130). Consequently, King (2010, p. 850) concludes that "cyberbullies feel protected by anonymity."

[4] According to Davenport (2002), anonymity weakens the behavioral constraints imposed by the criminal justice system, an effect that facilitates deviance because it minimizes the threat of being punished. As a result of the sense of anonymity, people often perceive cyberdeviance as having few repercussions (D'Arcy and Herath 2011).

Moving from costs to benefits, per differential reinforcement, the more an outcome is perceived on the basis of social learning as positive (e.g., as a *benefit*), the more likely it tends to encourage the modeled behaviors (Akers 1990). The extant cyberbullying literature also argues that offenders not only examine costs, but calculate benefits before they decide to commit such acts (e.g., Hemphill and Heerde 2014, Hinduja and Patchin 2013). Anonymity can also influence the perception of benefits, although this is often less tangible than costs. The basic idea is that anonymity allows offenders to experience benefits they would not experience nonanonymously. The direct benefits of cyberbullying vary from case to case; however, according to existing literature, these benefits generally include revenge, seeking social approval, having fun, attracting attention, asserting power/influence, and so forth (Miller 2013, Varjas et al. 2010, Xiao and Wong 2013). In the Ralph Espinoza case, the likely rewards were social bonding, power, and entertainment.

Regardless of the benefits imagined by bullies, we argue that anonymity increases imagined and/or real benefits. Likewise, anonymity can also give bullies more power and control, as has also been theorized in the early cyberbullying literature (Dooley et al. 2009). Later it was similarly theorized that cyberbullies benefit themselves through "a systematic abuse of power" (Slonje et al. 2013, p. 26) on their victims, and these external/internal benefits are magnified by increased power imbalance between the cyberbullies and the victims. Anonymity amplifies this imbalance. For example, in the online world, a number of different fake accounts can be created, which can be used for bullying the same or different victims (Galán-García et al. 2016). Social media via anonymity also provides many different ways to bully someone and thus achieve stronger benefits than is possible nonanonymously (e.g., anonymous versions of messaging, photos, fake people, memes, down voting, attachments, comments to a victim's friends, movies, and so on). In such an anonymous environment, with numerous ways to commit power-imbalanced attacks, victims are virtually powerless to protect themselves, which makes the cyberbullies' abuse of power more effective (Moore et al. 2012), and thus the more likely perceived benefits will result. Hence:

Hypothesis 3 (H3). *An increase in anonymity is associated with increased cyberbullying benefits.*

4.1.3. How Cyberbullying Anonymity Influences Definitions. Again, *definitions* refer to whether an action is good or bad (i.e., favorable or unfavorable) based on the learned attitudes, beliefs, and justifications for certain behaviors (Akers 1990). Moreover, the *neutralizing definition* is whether the deviant behavior can be justified as good. Here, definitions emphasize the inner values formed from past cyberbullying experiences that may further influence the justifications for performing such behaviors in the future. We continue to argue that cyberbullying anonymity shifts the social structure such that definitions are different than in the physical world, and this includes increased neutralizing definitions. One who has chosen to cyberbully is more likely to have defined and justified cyberbullying as generally favorable and acceptable, at least in a particular instance. In the Ralph Espinoza case, the bullies thought they were just having a "good time," and they were not aware of the severe psychosocial damage they were doing to him. (This is more likely with anonymity because there is a lack of two-way communication through which the victim's pain can be conveyed.) Worse, the longer it went on, the more normal and acceptable this routine was.

Previous research has argued that the high degree of anonymity in such environments increases the likelihood that cyberdeviant behaviors harmful to others "do not cause so many negative feelings (e.g., guilt, shame, self-condemnation)" (Pornari and Wood 2010, p. 89) for perpetrators and reduces "the chance of empathizing with the victim" (Robson and Witenberg 2013, p. 214). According to SSSL, by using neutralization techniques, criminals may accept deviant acts as "'all right' under certain conditions" (Akers 2011, p. 36).

SSSL applied to neutralization theory readily explains why such justifications are increased by anonymity. We posit that the structure of the online environment makes such "acceptable conditions" more readily available. For example, because of key anonymity subconstructs on social media—particularly, diffused responsibility, lack of proximity, and lack of knowledge of others—the perpetrator can hide, and the consequences of a cyberbullying act are difficult to see or measure. These factors allow cyberbullies to invoke neutralization techniques that involve *denial of responsibility* (Siegal 2011, Sykes and Matza 1957). Likewise, unlike physical bullying, it is hard to see the actual consequences of cyberbullying, especially if anonymity is involved and the victim thus cannot express their injury to the bully. This fosters the neutralization technique of *denial of injury* (Siegal 2011, Sykes and Matza 1957), among other likely neutralization techniques. We thus propose the following:

Hypothesis 4 (H4). *An increase in anonymity is associated with increased cyberbullying neutralization.*

Likewise, we argue that perceived anonymity on social media further modifies the social structure of the online environment by fostering moral disengagement, which in turn facilitates the learning of definitions that support cyberbullying. This increase in moral disengagement then results in increased neutralization and decreased situational morality, which is the mechanism that otherwise ethical people use to justify immoral behavior. *Moral disengagement* comprises "the mechanisms individuals activate to override the influence of their internal self-sanctions and to distance themselves from perceived reprehensible consequences of their behavior" (Garbharran and Thatcher 2011, p. 302). In the Ralph Espinoza case, even though the cyberbullying behaviors were abhorrent to others, the people involved were generally well behaved, moral, and professional in their day-to-day work. Once online, it was as if their dark alter egos took over their normal morality and skewed their behavior as normal, acceptable, and moral—even fun. Anonymity helped create this conundrum due to the lack of rich media and communication to understand the pain they were causing Espinoza.

We posit that moral disengagement is a natural consequence of disinhibition and deindividuation. Per Suler (2004), when individuals commit deviance in an online anonymous environment, their moral cognitive processes are often temporarily suspended. We argue that it is this that fosters positive moral definitions of deviate behavior. Pornari and Wood (2010, p. 89) argue that the high degree of anonymity in such environments increases the likelihood that cyberdeviant behaviors harmful to others "do not cause so many negative feelings (e.g., guilt, shame, self-condemnation)" for perpetrators, and Robson and Witenberg (2013, p. 214) argue that it reduces "the chance of empathizing with the victim." Thus, people find it easier to justify their deviant behaviors in response to criticism from others in anonymous online environments (Davenport 2002). Anonymity suspends normal forms of social interaction and social mores; thus, "problem behaviors may be recognized, rationalized, and mutually encouraged by others" (Ko et al. 2008, p. 575). According to Bauman and Pero (2011) and Gini et al. (2014), moral disengagement caused by online disinhibition results in disregard for social mores and morals. Thus:

Hypothesis 5 (H5). *An increase in anonymity is associated with decreased cyberbullying situational morality.*

4.2. How Social Learning Outcomes Influence Cyberbullying Frequency

NSI is especially apt in our context because in SLT, a criminal or delinquent actor models and imitates the deviant behavior (i.e., NSI) of fellow group members (Akers et al. 1979). Thus, a strong connection exists between NSI and crime (Kahan 1997). Related research has shown that if people belong to a group that promotes violence (i.e., NSI), they are more likely to assimilate such negative norms as less costly and more beneficial and engage in similar behavior (Bocij and McFarlane 2003). The cyberbullying literature has also begun to identify this link, primarily in connection with various forms of negative social norms and exposure (Hinduja and Patchin 2013). Imagine in the Ralph Espinoza case if employees or management had intervened early on and tried to socially shame the bullies. Instead, no one stood against the NSI. As a consequence, unchallenged NSI in cyberbullying groups strengthens the belief that cyberbullying is "cool," beneficial, or acceptable (DeHue et al. 2008), and thus encourages cyberbullying. In summary, if the SSSL model holds true in our context, then we hypothesize the following:

Hypothesis 6 (H6). *An increase in cyberbullying NSI is associated with increased cyberbullying.*

Next, we deal with the effects of perceived cyberbullying benefits and costs on cyberbullying frequency. These hypotheses should hold prima facie, based on the SSSL model, the SLT, and the previous hypotheses related to benefits and costs. SSSL and SLT posit that the observed benefits from a crime are linked with increased rates of a crime, and observed costs are associated with decreased rates of a crime. These are argued to hold also for the social media context and cyberbullying. Thus, when people experience differential reinforcement that artificially increases perceived cyberbullying benefits and decreases perceived costs, they are more likely to commit cyberbullying. This was certainly the situation in the Ralph Espinoza case, but the converse could also have been true—had there been any management oversight, positive peer pressure, or workplace punishments.

Hypothesis 7 (H7A). *An increase in cyberbullying benefits is associated with increased cyberbullying.*

Hypothesis 7 (H7B). *An increase in cyberbullying costs is associated with decreased cyberbullying.*

Neutralization theory (Sykes and Matza 1957) argues that neutralizations are linked to criminal behavior. A basic assumption of neutralization theory is that people who engage in delinquent behavior "believe in the norms and values of the community in general" (Siponen and Vance 2010, p. 489) but are temporarily suspending them by using neutralization techniques to avoid guilt. In the Ralph Espinoza case, the people involved in cyberbullying saw it as harmless fun and a way to "blow off steam." They did not recognize the immorality of their behavior or the psychosocial damage to Espinoza. Worse, the more people who joined in on the abuse, the more acceptable it became because "everyone was doing it."

Moreover, early neutralization theory studies have proposed a distinction between "acts that are wrong in themselves" and "acts that are illegal but not immoral" (Sykes and Matza 1957, p. 667); the former causes more guilt than the latter. Thus, nonsociopathic people feel guilty and ashamed when they realize their behaviors do not comply with ethical standards, which in turn prevents them from performing deviant behaviors, unless they morally disengage and neutralize such behaviors. Before engaging in delinquent behavior, people often justify it subjectively with neutralizing definitions, and certain neutralization techniques[5] help them to justify their delinquent behaviors as acceptable under the circumstances, thereby removing moral restrictions (Mitchell and Dodder 1980). Finally, a few studies have proposed that juveniles use neutralization when they choose to cyberbully (e.g., Bauman 2010, Renati et al. 2012), and given the above, this link likely extends to adults. Thus, we hypothesize the following:

Hypothesis 8 (H8A). *An increase in cyberbullying neutralization is associated with increased cyberbullying.*

Finally, because perceived anonymity leads to moral disengagement—which decreases situational morality—we continue this chain of logic to explain how increased situational morality decreases cyberbullying. Importantly, the evaluation of an act as morally wrong leads to avoidance of the action, especially when the person has the freedom to do so (Hare 1981). The converse is also true: when an action is regarded as morally acceptable, it is likely to be done, especially when the person has motivations to do so. We argue that the same reasoning holds for cyberbullying. Thus:

Hypothesis 8 (H8B). *An increase in situational morality is associated with decreased cyberbullying.*

5. Methodology

This study is the result of engaged scholarship (Van de Ven 2007) pursued over several years to build a model and gather empirical data to enhance the understanding of cyberbullying. We started with four preliminary studies, which were followed by two separate data collections that were part of the peer-review process for this manuscript. The present study represents the third data collection. Details of the other studies are available on request.

5.1. Data Collection and Advanced Sample Filtering to Improve Data Quality

The most challenging aspect of our research is that despite its pervasiveness, cyberbullying involves behaviors that are considered socially unacceptable in most cultures. We needed to study such behaviors in a manner that would elicit honest responses while maintaining anonymity. We chose to use an anonymous self-reported cross-sectional survey, which is strongly supported in the literature: Previous studies of deviant behaviors have effectively used cross-sectional studies in a variety of settings (e.g., Bennett and Robinson 2000, Higgins et al. 2008, Hinduja 2007, Lowry and Moody 2015, Lowry et al. 2015, Posey et al. 2015). SLT has also been examined by self-report studies conducted by its developers (Akers et al. 1979) and others (e.g., Higgins 2006, Higgins and Makin 2004, Skinner and Fream 1997, Winfree et al. 1994). Moreover, substantial IS research has used cross-sectional studies involving self-reported behaviors, in a greater variety of contexts (Karahanna et al. 1999, Lankton et al. 2010, Moody and Siponen 2013, Vance et al. 2012, Venkatesh et al. 2012).

The use of self-reports may involve social desirability bias, which we took the following measures to reduce: First, we provided the respondents with a certain level of anonymity. To ensure anonymity between the respondents and researchers, we used a third-party online panel. Consequently, the respondents never interacted with the researcher, and the researcher never had access to the respondent's contact information, which is a leading practice to thwart social desirability bias (Awad and Ragowsky 2008, Lowry et al. 2013, Posey et al. 2013). Using the specific panel of Mechanical Turk (MTurk) also allowed us to gather respondents from a wide range of sociodemographic backgrounds, people who would have been virtually impossible to reach otherwise. MTurk is a particularly useful platform for such studies because millions of people are registered to respond, and the platform allows for advance-screening measures, which are helpful in recruiting people with preferred characteristics.

We followed the latest methodological literature on MTurk (e.g., Goodman et al. 2013, Landers and Behrend 2015, Lowry et al. 2016, Steelman et al. 2014) and used it in combination with advanced survey features and filtering through Qualtrics online surveys, which greatly improved the data quality (e.g., Goodman et al. 2013, Landers and Behrend 2015, Lowry et al. 2016). This literature indicates that our data collection context was an especially good fit for MTurk; it is a topic of general interest for which no special expertise was needed, the data could be collected with reasonable assurances of anonymity, and

[5] Examples of neutralization techniques to justify behaviors include denial of responsibility, denial of injury, denial of the victim (i.e., denying the existence of a real victim), condemnation of the condemners, appeal to higher loyalties (Sykes and Matza 1957), the metaphor of the ledger (Klockars 1974), and the defense of necessity (Minor 1981). These techniques have been thoroughly studied, and several others are likely applicable to cyberbullies. We thus conducted a full review of these techniques and summarized 14 relevant neutralization techniques from the literature (available on request). However, which techniques are chosen in various scenarios is not as theoretically important for the SMCBM as the general proposition that if the SLT/SSSL model holds in this context and is driven by NSI, the definitions factor of SLT is likely to be strongly represented by neutralization by those who choose to cyberbully, often against their better moral judgment. For this reason, as well as for theoretical concision, we depict neutralization as a second-order construct, which is consistent with the theoretical models developed by Jarvis et al. (2003) and Siponen and Vance (2010).

it is an ideal way to reach a large number of people with specific traits (e.g., having committed cyberbullying). First, we employed multiple screeners (including IP address and geolocation information) to ensure that only English-speaking adult respondents who lived in the United States could take the survey (the same country and language were required for consistency in the laws and norms regarding social media). The respondents were also required to have had committed at least one act of cyberbullying on social media in the last year and to have been willing to provide their opinions about cyberbullying in general. To eliminate (semi)professional survey takers, we used the MTurk's screening capabilities to make the survey known and available only to people who had taken a maximum of three previous surveys. However, we also paid a reasonable amount of compensation such that participants had the reasonable opportunity to earn around U.S. minimum wage per hour. We also used Qualtrics' technical option to prevent more than one response from the same IP address.

In view of the length and sensitive nature of the survey, to decrease monomethod bias and increase both honesty and attention, we implemented the following procedural remedies taken from the literature (e.g., Goodman et al. 2013; Landers and Behrend 2015; Lowry et al. 2013, 2016; Rouse 2015; Steelman et al. 2014) that have been shown to address these issues: (1) we randomized the order of the survey questions; (2) we reversed the scaling and anchors of half of the survey questions; (3) we used questions with different anchors; (4) we combined questions that were each other's opposite or were unrelated; (5) we implemented randomly presented attention-trap questions to ensure that the respondents were reading and understanding the questions; (6) we asked the respondents to verify their honesty and completeness in answering; (7) we explained the importance of paying attention and the scientific importance of the study; (8) we tracked the time spent in completing the surveys and eliminated any that were taken unusually fast compared to our pilot tests; (9) we provided data validation, look-ups, and other survey screeners to improve data accuracy; and (10) aside from these efforts, which help to prevent common-method bias a priori, we gathered a marker variable per Richardson et al. (2009), which in our case was based on organizational commitment and provides additional evidence for the absence of common method bias.

5.2. Data Filtering and Sociodemographic Data

Following the leading practices for MTurk studies that involve lengthy surveys, we employed a high degree of filtering to ensure a high degree of data quality; this is because such studies are prone to high dropout rates and attempts to rush through the survey.[6] The sociodemographic data of the 1,003 respondents were as follows: age ($\bar{x}$, 31.02 years; SD, 8.36), first year on the Internet ($\bar{x}$, 1999; SD, 4.00 years; min., 1993; max., 2012), and work years ($\bar{x}$, 12.00 years; SD, 8.27). The gender distribution was 514 males (51.2%), 483 females (48.2%), and 6 other genders (0.6%). The respondents' employment distribution was as follows: 185 full-time students (18.4%), 92 unemployed and nonstudents (9.2%), 162 employed part time (16.2%), and 564 employed full time (56.2%). Full details of all demographics and individual cyberbullying behaviors are presented at the end of Online Appendix D.

5.3. Measures and Controls

All measures were based on established measures and were modified to fit our cyberbullying context where necessary. Here, we supply details on how some of our key constructs were measured to illustrate important aspects of our measurement strategy. Full details

[6] A total of 1,972 people on MTurk saw our human intelligence task (HIT) and examined the disclosure page of our survey. Fifty people indicated they had never committed cyberbullying and thus were disqualified, and 167 people decided to not continue with the study or refused to provide consent, leaving 1,755 people who went to the first page of the survey, the demographics section. When asked for their country, five people indicated they did not live in the United States, even though their IP address indicated a U.S.-based computer, and thus were eliminated. Another 156 people did not continue at this point, leaving 1,594 people who went to the next page of demographics. Another 27 people dropped out at this point, leaving 1,567 people. Because of the length of the survey, we then randomly provided five attention-trap questions throughout the remainder of the survey to ensure the respondents were being honest, were paying attention, and were not rushing through the survey. The first trap caught 205 people off guard, who were removed, after which 20 people decided to not complete the IT artifact section, leaving 1,342 people in the study. After this, they were given instructions about the cyberbullying section and reminded of the requirement to disclose their cyberbullying behaviors. One hundred forty-two people did not continue, leaving 1,200 people. In the final sections of the survey on cyberbullying behaviors, four more attention traps were executed. Trap 2 was provided in this section of the survey, causing 61 people to be removed, leaving 1,139 people. Thirty-four people did not pass Trap 3, leaving 1,105 people. Nineteen people did not pass Trap 4, leaving 1,086 people. Thirteen people did not pass Trap 5, leaving 1,073 respondents. Another 70 people passed all of the attention traps but did not fully respond to all cyberbullying behavior questions, and thus they were dropped, leaving 1,003 respondents for the final data analysis. Finally, the attention trap questions that were used were the following:

1. It is true that Donald Trump has unusual hair.
2. If adding two to the number three equals five then only select "somewhat agree" and nothing else.
3. If adding two to the number six equals eight then only select "neutral" and nothing else.
4. If you have been answering honestly thus far, please only select "agree" and nothing else.
5. It is true that Hillary Clinton used to be the President of the United States.

Table 2 Prompt, Scaling, and Measurement Items for Cyberbullying Anonymity

Prompt: You indicated that you have used [social media] in the past year for cyberbullying. We would like to know your beliefs about using [social media] for cyberbullying. When cyberbullying other people using [social media], which of the following best describes your opinions about [the social media itself] in bullying others? "I believe that…"

Scaling: 7-point Likert-type scale anchored on 1 = very strongly disagree…7 = very strongly agree.

(A-LI1) …my personal identity won't be provided.
(A-LI2) …my cyberbullying is entirely secret.
(A-CS1) …the system(s) will not identify me without my permission.
(A-CS2) …no names will be attached to the systems' internal records unless that is what I want.
(A-DR1) …it is impossible to make me more accountable than others for cyberbullying.
(A-DR2) …it is impossible to blame me personally for any cyberbullying.
(A-PX1) …others can't physically see what I am doing on my computer screen (e.g., walk by and see what I'm writing).
(A-PX2) …I feel assured that no one can physically observe me in the act of cyberbullying (e.g., look over my shoulder when I'm typing).
(A-KO1) …my behavior(s) do NOT have enough distinguishing characteristics that would allow other people to identify me as the originator of the cyberbullying.
(A-KO2) …it is impossible to identify me as the origin of the cyberbullying based on my personal characteristics.

Notes. The cyberbullying anonymity measures were modified from social anonymity measures by Lowry et al. (2009). Social anonymity is a second-order factor composed of the following reflective constructs: lack of identity (A-LI); confidence in the system (A-CS); diffused responsibility (A-DR); proximity (A-PX); and knowledge of others (A-KO).

on measurement, with sources, controls, prompts, and survey logic are in Online Appendix C.

To measure *cyberbullying anonymity*, we asked respondents to answer questions with respect to the social media platform they had most used for cyberbullying, the idea being that the level of anonymity can vary across platforms and even within a particular platform depending on a person's use patterns (see Table 2 for details). To measure *cyberbullying frequency*, we again asked them to answer with respect to the platform they had most used for cyberbullying, and to disclose the frequency (i.e., never, one time, monthly, weekly, daily) with which they had engaged in each of four behaviors: (1) post something hurtful, rude, inappropriate, or mean that targets someone; (2) publicly embarrass or prank someone with true information or photos that are potentially harmful; (3) spread a rumor or untrue information about someone; (4) send threatening or harassing messages, or send messages after someone told you to stop. To measure the SLT variables, we again asked respondents to answer with respect to the platform they had most used for cyberbullying. We also had them answer these questions separately for each of the four cyberbullying behaviors, the rationale being that a respondent's perceptions could vary across the different cyberbullying behaviors. For example, the perceived costs and benefits of "posting something hurtful" could be different from those for "sending threatening or harassing messages." The neutralizations used to justify "publicly embarrassing or pranking someone" could be different from those for "spreading a rumor or untrue information."

6. Analysis and Results

For model analysis, we used partial least squares (PLS) regression using SmartPLS version 2.0 (Ringle et al. 2005). Because PLS is especially adept at the validation of mixed models of formative and reflective indicators, it is more appropriate than covariance-based structural equation modeling for preliminary model building, and it is ideal for large models (Chin et al. 2003, Gefen et al. 2011, Lowry and Gaskin 2014).

We first conducted preanalysis and data validation for four purposes: (1) to establish the factorial validity of the measures through convergent and discriminant validity, (2) to establish that multicollinearity was not a problem for any of the measures, (3) to check for common-method bias, and (4) to establish strong reliabilities. Details are given in Online Appendix D. Figure 3 shows the final results of all paths and controls. The full details are available in Table D.5 in Online Appendix D.

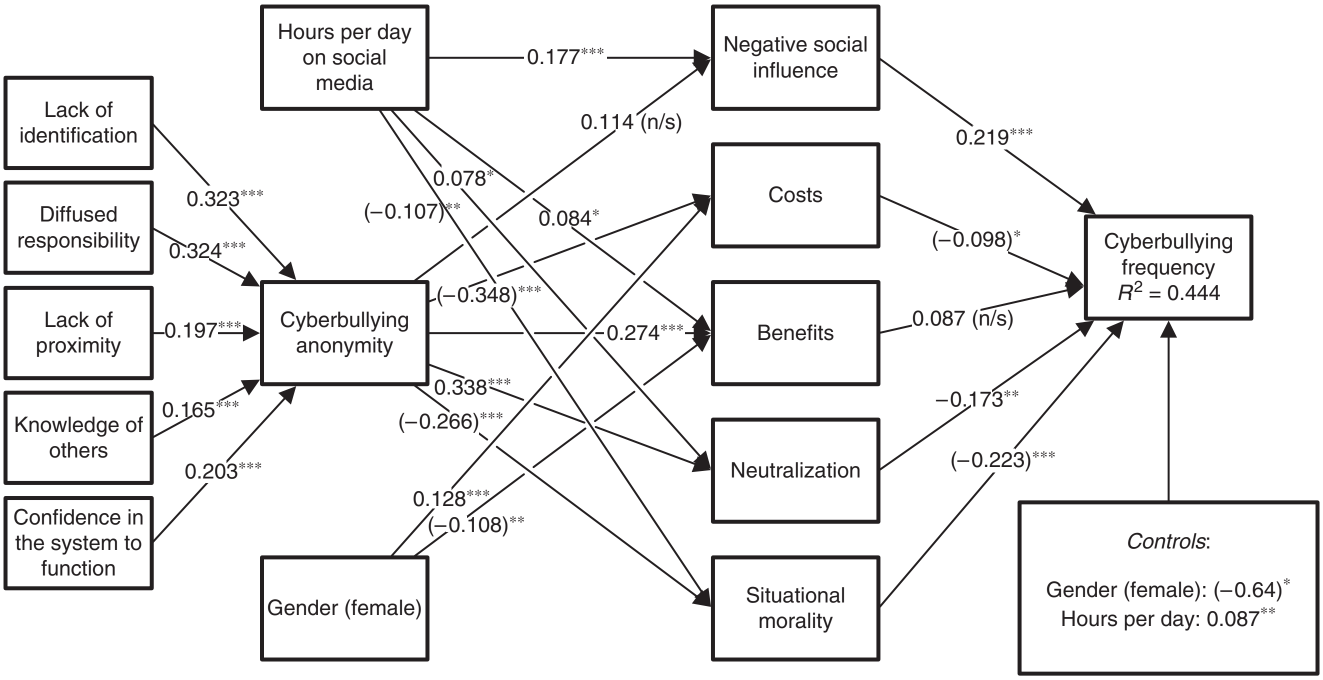
We also used bootstrapping techniques to test for mediation in our model (see Online Appendix D). We confirmed that our model follows the core SSSL model prediction, in which all social learning constructs act as full mediators. We are the first to show the rich second-order construct of cyberbullying anonymity as a direct driver of cyberbullying that is fully mediated by social learning constructs.

7. Discussion

7.1. Summary of Results

Most of our hypotheses were supported. The association between anonymity and NSI was significant in the initial model but became insignificant when hours per day on social media was added (H1 rejected). Anonymity was associated with decreased costs (H2 supported), increased benefits (H3 supported), increased neutralization (H4 supported), and decreased situational morality (H5 supported). NSI was associated with increased cyberbullying (H6 supported).

Figure 3 **Model Results with Controls and Exploratory Relationships** ($n = 1{,}003$)



Notes. This figure includes all hypothesized paths, but only significant control paths. n/s, not significant.
$^{*}p < 0.05$; $^{**}p < 0.01$; $^{***}p < 0.001$.

Costs were associated with decreased cyberbullying (H7A supported), but benefits were not associated with increased cyberbullying (H7B rejected). Neutralization was associated with increased cyberbullying (H8A supported), and situational morality was associated with decreased cyberbullying (H8B supported).

We also explored several traditional sociodemographic factors that have influenced social learning constructs in more traditional criminal and deviance research (Akers 2011). We also ran the same factors as control variables against cyberbullying frequency, including age, gender, education, employment status, income, and hours per day on social media. We were surprised by how few of these influenced any of the social learning constructs or cyberbullying frequency, although this is another indicator that the social media community context is indeed unique: social structural correlates of the physical world cannot represent the social structure of one's network characteristics in social media. In terms of significant structural correlates, being female was associated with decreased cyberbullying benefits and increased costs; hours per day on social media was associated with increased cyberbullying NSI, increased benefits, increased cyberbullying neutralization, and decreased situational morality. There were no effects associated with age, education, employment, or income. In terms of the control variables, hours on social media was associated with increased cyberbullying frequency. Being female was associated with decreased cyberbullying frequency, whereas age, education, income, and employment status had no influence on cyberbullying frequency. Again, this is interesting in an SLT context, where such sociodemographics often matter.

7.2. Interpretation of Results and Contributions

Our study provides several key contributions to the understanding of adult cyberbullying. First, we examined to what extent the SSSL model can account for cyberbullying, and we also revised the SSSL model to account for the unique social media community environment that is fostered by perceived anonymity and its associated causal mechanisms of disinhibition and deindividuation. We show that few of the traditional environmental criminological factors apply online and that the social learning mechanisms are instead largely driven by three factors: the richly conceptualized factor of perceived anonymity (i.e., lack of identification, diffused responsibility, lack of proximity, knowledge of others, and confidence in the system to function), hours per day spent on social media, and gender. Hence, the SMCBM is a compelling model to use to study cyberbullying, especially when social learning and environmental influences are of utmost concern.

We are also among the first to examine more than one specific cyberbullying behavior in either an SSSL model or an SLT study, and we are the first to provide a social learning micro- and macroperspective on cyberbullying. Examining four major sets of cyberbullying behavior allowed for a more robust and generalizable test of the SMCBM. We employed a novel survey-only design in which each unique cyberbullying behavior was randomly ordered (to cancel out any ordering effects), and the respondents provided social learning responses to one specific form of cyberbullying at a given time. Although it made sense in traditional SLT/SSSL studies to examine one behavior because other behaviors are unrelated (e.g., larceny, alcoholism, elder abuse, and shoplifting), we argue this is not the case with cyberbullying because it involves a lot of related but distinct behaviors. Thus, we believe that providing a set of four commonly committed types of cyberbullying provides a stronger, more realistic, and more generalizable test of our SMCBM than if we had chosen one form of cyberbullying (e.g., sending a malicious message, saying something hurtful, passing on a malicious rumor, or intentionally embarrassing someone).

Moreover, to robustly test the SMCBM, we tested for mediation using advanced bootstrapping techniques. These results are detailed in Online Appendix D. We thus are able to demonstrate that the influence of cyberbullying anonymity on cyberbullying frequency is fully mediated by the social learning constructs. This further shows that the SMCBM model fits the underlying theoretical assumptions of the SSSL model; that is, the social learning constructs are mediators, and the causal ordering matters. This hopefully sets the foundation for additional research that involves more direct testing of causality and longitudinal effects.

Notably, unlike traditional SSSL models involving criminology, there were no social learning effects associated with age, education, employment, or income, which are often associated with traditional crimes (Akers 2011). We explain this difference by the contextual differences between the physical world and the unique context of social media. For example, in the physical world, lack of employment and low income may motivate some people to commit crimes to earn money (Sutherland 1947). Moreover, the type of social media platforms our respondents engaged in were generally socially based and not associated with financial opportunities. Education might be able to prevent crimes in the physical world by inculcating values that favor social norms against crimes. Indeed, research has argued that many of our moral values are established through upbringing and education and evolve over time (Hare 1981, Kohlberg 1981). Thus, it may be that the inculcation of values against cyberbullying through educational institutions has either not taken hold of today's adults or they have never received this education.

However, we do find a strong social learning effect with hours per day on social media—so much so that when it was added to the baseline model, it predicted NSI and anonymity dropped out. Our interpretation is that from a social structure standpoint, the amount of time spent on social media much more greatly influences whom one associates with who is committing deviant behaviors than does anonymity. Time matters, because it shifts one's social structure increasingly from offline to online. Moreover, much abusive, socially modeled behavior can be easily witnessed without anonymity. However, further research on this is needed because hours per day on social media was a one-item measure. There also could be measurement issues in differential association because our formative measure mixed two different kinds of scaling (norms and frequency).

We also found a strong gender effect that we did not expect or predict. Females in our sample were significantly less likely to commit cyberbullying than males. Moreover, females perceived fewer benefits and more costs of cyberbullying than did males. Hence, there may be strong social learning differences in cyberbullying behavior based on gender, including how costs and benefits are interpreted. Some of this could likely have to do with a key motivating factor of cyberbullying: that of control and power imbalance between the bully and the victim (e.g., Moore et al. 2012, Slonje et al. 2013). These results may also relate to differences in genders based on aggression. Although the stereotype is that men are more aggressive than women, the reality is more complex. Older meta-analysis shows that men tend to be more aggressive in terms of physical harm, but not in terms of social or psychological harm (Eagly and Steffen 1986). Interestingly, the same research does show that women are more likely to perceive harm to the victim, guilt, anxiety, and danger to oneself when envisioning performing an aggressive behavior. These factors need further research in respect to cyberbullying.

As noted earlier, although cyberbullying is acknowledged as a serious issue with juveniles, it is also a serious issue with adults (Nycyk 2015). However, prior to this study, little was known about how to predict and discourage this behavior in adults or about their actual cyberbullying patterns and social media choices. As a new generation of social media users—who grew up as digital natives and have routinely practiced cyberbullying as a rite of passage—enters the workforce, many are bringing these pernicious, socially learned behaviors with them. Of concern is our finding that our adult respondents use neutralization to suspend normal, rational judgment when choosing to engage in cyberbullying, because they likewise decrease perceived costs, increase perceived benefits, and suspend their offline moral inclinations. Worse, it is the characteristics of social media itself (e.g., perceived anonymity) combined with hours per day on social media that create this toxic condition. The behaviors we report involve not only minor harassment and rudeness but also harmful actions that can lead to reduced work productivity, social strain, psychological trauma, criminal behavior, job loss, and lawsuits—as in the Ralph Espinoza case.

Moreover, the role of social media providers as enablers of cyberbullying requires further attention, and our work in laying out the rich construct of perceived anonymity is only a starting point. Certainly, Facebook stands out as the chief adult cyberbullying platform, but our results show that adults use several other channels (e.g., Reddit, YouTube, Twitter, Instagram, and Disqus). We show that certain social media artifacts make cyberbullying easier, which helps explain why corresponding physical behaviors (e.g., bullying and stalking) in adults are not as prevalent. Social media artifacts can inspire disinhibition and deindividuation, which make adults feel more comfortable performing deviant behaviors online than offline, and social media providers are largely responsible for the design of the IT artifacts and system conditions that create disinhibition and deindividuation. We assume that these conditions are especially worsened by social media artifacts intentionally designed for anonymity, such as allowing self-destructing messages, nonidentified users, multiple accounts at the same IP address, easy access to "friends of friends," not monitoring access from known IP-masking services, not requiring human moderators, and not having bots that monitor behavior.

7.3. Limitations and Future Research Directions

Our study focuses on the "dark side" of social media and thus lacks an emphasis on positive aspects that prevent people from being involved in cyberbullying. It is thus particularly important to better understand what prevents Ralph Espinoza cases from happening in the first place, such as positive conforming behavior in the workplace. First, SLT suggests that association with nondeviant peers can also lead people to perform conforming behaviors against cyberbullying (Akers 2011). In some real-world cases, role models against workplace cyberbullying play an important role in allowing colleagues to learn conforming rather than deviant behavior (XpertHR 2012). Second, companies can cultivate employees' positive conforming behavior and adopt measures to thwart and punish cyberbullying. In some cases, employees must be fired to protect the work environment. For example, a call-center employee made offensive Facebook comments about a colleague, and the employee was fairly dismissed even after appealing the case (XpertHR 2012). In addition, the U.S. government has developed a one-stop shop of tools at Stopbullying.gov that emphasizes use of social networking features to prevent cyberbullying behaviors (Woda 2013). Thus, future research should consider positive aspects of social media that can help people leverage a positive social learning process of antibullying behaviors and examine how IT artifacts themselves can help prevent cyberbullying behaviors.

The SMCBM is intended to maximize prediction of adult cyberbullying frequency, as modified from the SSSL model. Nonetheless, the SMCBM contains more inferred causality than can be tested with cross-sectional data, because it has been explained by factors such as the causal mechanisms of disinhibition and deindividuation. As with a typical variance model, causation can be inferred primarily from the theoretical explanation, but little such causation can be demonstrated on the basis of our form of testing, other than through the mediation testing we conducted. Likewise, the nature of our measurement design does not allow for a distinction between initial and ongoing deviance. Our model implicitly assumes that most of the participants' deviance is ongoing, such that they are not new to cyberbullying. It would be particularly interesting to study people who had just committed their first and only act of cyberbullying to better understand the imitation process, but this is especially challenging because of sampling constraints. Akers et al. (1979) found that imitation was important in explaining one's very first act of deviance; after that, it had virtually no predictive effect on ongoing deviance. For these reasons, we did not include imitation in our model.

Consequently, other methodologies should be employed to further build this area of research; however, this is easier said than done in social learning and SSSL model research. For example, experimentation is probably the most problematic solution and has yet to find much success in such studies. Researchers have previously found it difficult to obtain results by using short-term experimentation in this context (Pratt et al. 2010). We believe the reason for this is straightforward: Social learning is a process that takes time, and it is thus unrealistic to expect that an artificial manipulation will cause immediate changes. Social learning is not one event (unlike a fear appeal or other classic "interventions"); it requires continuous observation/imitation during a longer time period (Akers 2011). This is why cross-sectional studies are preferred over experimentation in this literature: cross-sectional studies can at least take snapshots of where a given person is at a given point in time in the social learning process. Moreover, our context is inherently social, involving interactions with large numbers of people over time. How to emulate this in a realistic manner in a short-term experiment has yet to be determined.

Because social learning is a process, longitudinal studies of cyberbullying are more promising than one-time experiments. In SLT/SSSL research, some longitudinal studies have been conducted, but these are especially challenging in deviance studies because it is difficult to find participants willing to disclose potentially criminal behavior over time (causing a stronger self-selection bias), and such studies are prone to high dropout rates. Moreover, longitudinal studies are difficult to execute without full identification of the participants because the researchers must ensure that the right data are mapped to the right person. Such identification undermines anonymity, which then foster responses that are prone to social desirability bias. Another challenge of these studies is that the social learning processes for cyberbullying may require years of exposure. Nevertheless, this is an important future direction for cyberbullying research.

Although we had a large number of respondents from a diverse sociodemographic range, our study cannot be assumed to be widely generalizable. First, we allowed only U.S. respondents to ensure similarity with respect to assumed laws and national cultural mores. We expect that cyberbullying in countries with heavy social and governmental monitoring and different cultural norms would take on nuanced forms and might have different foci in the social learning constructs. Cross-cultural IS research in other contexts has been informative (e.g., Lowry et al. 2011, Posey et al. 2010); thus, testing the SMCBM in places such as China, India, Indonesia, Russia, Egypt, Brazil, South Africa, Nigeria, and Mexico would likely be informative.

It is also important to note that our study had a self-selection bias, which is difficult to estimate. In our case, the respondents were those who willingly and anonymously disclosed their cyberbullying behavior. Thus, it is theoretically possible that those who remain silent about their cyberbullying may experience other, more influential factors of which we are not aware (e.g., a greater sense of shame or more self-control). Furthermore, we cannot infer that these results transfer to juveniles because of differences in moral development, but we still believe that applying the SMCBM to them would be a useful starting place because much of the model will likely hold.

Again, we tested common sociodemographic factors that have been used in SLT/SSSL deviance studies, and most of these were insignificant. Going forward, other explanations for cyberbullying should be explored and added to the SMCBM. For example, a potential explanation is one's lack of self-control or propensity to anger and under which conditions such predispositions lead to cyberbullying. Power is another example of a promising area for further theorizing and research. The physical power differential between the victim and offender has recently been reported to be important in traditional bullying but not in cyberbullying (Barlett et al. 2016). However, there may still be kinds of power or status effects that matter in cyberbullying.

Despite its social and technological importance, adult cyberbullying is overlooked in research (Nycyk 2015) and is generally ignored in management practice, even though much cyberbullying occurs at work or among coworkers (Baum et al. 2009). In fact, we found no previous studies involving participants over an average age of 25. As a result, adult cyberbullying remains unstudied, even though it is a pressing social problem and a dark side of the Internet (Nycyk 2015). We showed that the SMCBM works well to explain adult behavior, and that it appears that key factors such as situational morality, neutralization, negative social influence, and costs/benefits must be accounted for. However, given this useful baseline, more research must be conducted to see just how adolescents and adults differ, which will require future SMCBM data collections and modifications for adolescents. For example, research has shown that moral decision making develops over time and can thus differ between juveniles and adults (Kohlberg 1981). Research has also shown that juveniles are more prone to engage in risky behaviors and are more likely to be pressured into such behaviors than adults because adults can better estimate long-term consequences than juveniles (Gardner and Steinberg 2005). Thus, it may be that adults will have stronger situational morality considerations, and juveniles may be more affected by low self-control.

Another limitation is that for simplicity of modeling and measurement, we aggregated the four main types of cyberbullying in our main model; that is, we used an average of perceptions related to four related but different behaviors to predict the average level of those behaviors. To further address this concern, we conducted a sensitivity analysis of running four separate models for the four different behaviors (summarized in Table D.8 in Online Appendix D). The results across all four models were highly similar to our overall model, showing that the SMCBM holds well across different behaviors. However, there are many other specific forms of cyberbullying that require further investigation for which we cannot claim our model to hold and that may create more varied results, such as sexting, breaking into another person's computer for revenge, sending unwanted porn to someone, defacing a person's social media site, and so on. Other more advanced methodologies—such as multilevel modeling and hierarchical linear modeling—may also be useful when dealing with such highly disparate cyberbullying behaviors.

Moreover, although benefits was supported in our baseline model, it dropped out when the control variables and social media and structure factors were added. Hence, we cannot conclude benefits should not be included in the SMCBM; it just appears to be a weaker factor than costs. We suspect this may have to do with the nature of self-report in that costs of cyberbullying are likely easier to envision than benefits. For example, it is likely easier to envision getting caught than visualizing the benefits of power imbalance.

Notably, we measured costs and benefits more generally, as is often the case in RCT applications to deviant behaviors (e.g., Bulgurcu et al. 2010, Hu et al. 2011), so that our adult respondents could best define what they considered to be costs and benefits for themselves. This assumption is particularly useful for social learning, because costs and benefits are learned and not necessarily entirely rational or predictable across all forms of cyberbullying. Consequently, when people experience positive consequences of cyberbullying, such experiences reinforce their intention to cyberbully. Future research could benefit from the examination of specific costs and benefits of adult cyberbullying, and how these come about.

Finally, in concision, we focus on the five subconstructs of perceived anonymity that are the most likely drivers of the causal mechanisms of disinhibition and deindividuation in cyberbullying contexts. However, it is worthwhile to investigate other social media design considerations that may further drive or work in parallel with anonymity and to establish how they are different. This could include factors such as degree of synchronicity, media richness, and perceptions of monitoring. Moreover, future research should consider actual social media artifacts that could blunt cyberbullying, such as interfaces that are designed to increase accountability, social presence, and personal identity. Research should also account for the fact that people are increasingly using technologies external to social media (e.g., IP masking, virtual private networks (VPNs), and bit bleachers) to increase the anonymity of their social media interactions. In Table 3, we map many of the various social media design choices and technical factors that could have positive (+) and negative (−) influences on the five major factors of anonymity. At this point, these ideas are mostly speculative and need more theoretical development because little literature exists to support these relationships. Vance et al. (2015) showed a novel way that high volumes of IT artifact designs can be tested in a behavior security setting. We believe such an approach could be extended to study social media IT artifacts involved

Table 3 **Social Media Artifacts and Contextual Factors That Can Change Cyberbullying Anonymity**

	The five subconstructs of perceived cyberbullying anonymity				
Social media artifact and contextual factors	LI	DR	LP	KO	CS
Social media anonymity influencers that can be chosen in most social media systems					
Interacting only with strangers	+	+	+	+	
Interacting with real-world associations	−	−	−	−	
Using a small social community with largely known people	−	−		−	
Using a large social community with largely unknown people	+	+		+	
Communicating untrue details or using inauthentic personas	+		+	+	
Using one's true identity	−	−		−	−
Using pseudonyms	+	+			
Using asynchronous features to "buy time" to plot responses	+	+		+	+
Using different accounts and identities for different activities and goals	+	+		+	+
Social media anonymity influencers that exist only in some social media systems					
Using throwaway accounts	+	+			+
Using avatars	+	+		+	
Disallowing the creation of more than one account from the same IP address	−	−	−		−
Interacting with real-time video conferencing	−	−	−	−	−
Interacting with real-time instant messaging	−	−		−	−
Allowing users to easily report bad behavior or malicious comments	−	−			−
Requiring background checks and authentication of identity before joining	−	−	−	−	−
Using a social media system that is designed to conceal true identities[a]	+	+	+	+	+
Sending self-destructing messages		+		+	+
Allowing access to friends of friends		+	+	+	
Using a social media system that has automatic behavior-monitoring bots	−	−		−	−
Using a social media system that has human moderators or censors	−	−		−	−
Technical techniques that can be used with browsers or apps to increase cyberbullying anonymity					
Using IP-masking software or VPN	+	+	+		+
Blocking third-party cookies	+	+			+
Blocking location data	+	+	+		+
Using anonymous browser or do-not-track functions	+	+	+		+
Blocking plug-ins and JavaScript	+				+
Using encrypted connections	+	+	+		+
Using prepaid "burner" cell phones bought with cash	+	+	+		+
Bit-scrubbing and history-scrubbing software	+		+		+

Note. LI, Lack of identification; DR, diffused responsibility; LP, lack of proximity; KO, lack of knowledge of others; CS, confidence in the system.
[a]Examples of social media systems designed to conceal identities include Whisper, Yik Yak, and After School.

with cyberbullying. This alone provides an agenda for future cyberbullying artifact research and further illustrates the uniqueness of the social media context.

8. Conclusion

Whereas most cyberbullying research focuses on exploratory studies of juveniles or college students, ours is the first to focus on adult cyberbullies. Using engaged scholarship, we propose the SMCBM to integrate the inconsistent knowledge of drivers of cyberbullying with a recontextualization of the SSSL model that includes the social media artifact of perceived anonymity as a key social structure driver of cyberbullying. The SMCBM was largely supported, implying that the social media artifact of anonymity, along with hours of social media use per day, helps to drive the social learning process and that this process is largely responsible for adult cyberbullying. We thus offer the SMCBM as a comprehensive model—the first to include micro and macro components of social learning—for further research on adult cyberbullying and as a potential theoretical starting point for research on juvenile cyberbullying.

Supplemental Material

Supplemental material to this paper is available at https://doi.org/10.1287/isre.2016.0671.

Acknowledgments

The authors are especially grateful and indebted to the senior editor of this manuscript, who thoughtfully and patiently oversaw the development of this manuscript. The authors are also grateful to the editors for organizing the special issue workshop at Boston College, which also benefited this work. The authors also thank Tailai Wu for earlier work he contributed to this project. Finally, the authors acknowledge partial financial support for this project from the City University of Hong Kong and the University of Jyväskylä.

References

Acohido B (2013) Cyberbullying extends to workplace, bedroom. *USA Today* (February 18). http://www.usatoday.com/story/tech/2013/02/16/cyberbullying-workplace-romantic-couples/1887801/.

Ajzen I (1991) The theory of planned behavior. *Organ. Behav. Human Decision Processes* 50(2):179–211.

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

Akers RL (1990) Rational choice, deterrence, and social learning theory in criminology: The path not taken. *J. Criminal Law Criminology* 81(3):653–676.

Akers RL (1998) *Social Learning and Social Structure: A General Theory of Crime and Deviance* (Northeastern University Press, Boston).

Akers RL (2011) *Social Learning and Social Structure: A General Theory of Crime and Deviance*, 2nd ed. (Transaction Publishers, New Brunswick, NJ).

Akers RL, Sellers CS (2004) *Criminological Theories: Introduction, Evaluation, and Application*, 4th ed. (Roxbury Publishing, Los Angeles).

Akers RL, Krohn MD, Lanza-Kaduce L, Radosevich M (1979) Social learning and deviant behavior: A specific test of a general theory. *Amer. Sociol. Rev.* 44(4):636–655.

Akers RL, La Greca AJ, Cochran J, Sellers C (1989) Social learning theory and alcohol behavior among the elderly. *Sociol. Quart.* 30(4):625–638.

Awad NF, Ragowsky A (2008) Establishing trust in electronic commerce through online word of mouth: An examination across genders. *J. Management Inform. Systems* 24(4):101–121.

Baggili I, Rogers M (2009) Self-reported cyber crime: An analysis on the effects of anonymity and pre-employment integrity. *Internat. J. Cyber Criminology* 3(2):550–565.

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

Barlett CP, Gentile DA (2012) Attacking others online: The formation of cyberbullying in late adolescence. *Psych. Popular Media Culture* 1(2):123–135.

Barlett CP, Gentile DA, Chew C (2014) Predicting cyberbullying from anonymity. *Psych. Popular Media Culture* 5(2):171–180.

Barlett CP, Prot S, Anderson CA, Gentile DA (2016) An empirical examination of the strength differential hypothesis in cyberbullying behavior. *Psych. Violence* Forthcoming.

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

Bauman S (2010) Cyberbullying in a rural intermediate school: An exploratory study. *J. Early Adolescence* 30(6):803–833.

Bauman S, Pero H (2011) Bullying and cyberbullying among deaf students and their hearing peers: An exploratory study. *J. Deaf Stud. Deaf Ed.* 16(2):236–253.

Becker G (1968) Crime and punishment: An economic approach. *J. Political Econom.* 76(2):169–217.

Bennett RJ, Robinson SL (2000) Development of a measure of workplace deviance. *J. Appl. Psych.* 85(3):349–360.

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

Bocij P, McFarlane L (2003) Cyberstalking: The technology of hate. *Police J.* 76(3):204–221.

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

Burgess RL, Akers RL (1966) A differential association-reinforcement theory of criminal behavior. *Soc. Problems* 14(2):128–147.

Calvete E, Orue I, Estévez A, Villardón L, Padilla P (2010) Cyberbullying in adolescents: Modalities and aggressors' profile. *Comput. Human Behav.* 26(5):1128–1135.

Chin WW, Marcolin BL, Newsted PR (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. *Inform. Systems Res.* 14(2):189–217.

Clear TR, Rose DR, Waring E, Scully K (2003) Coercive mobility and crime: A preliminary examination of concentrated incarceration and social disorganization. *Justice Quart.* 20(1):33–64.

Cooper RM, Blumenfeld WJ (2012) Responses to cyberbullying: A descriptive analysis of the frequency of and impact on LGBT and allied youth. *J. LGBT Youth* 9(2):153–177.

Cohen AK (1955) *Delinquent Boys: The Culture of the Gang* (Free Press, Glencoe, IL).

Cressey DR (1960) Epidemiology and individual conduct: A case from criminology. *Pacific Sociol. Rev.* 3(2):47–58.

Crutchfield RD (1989) Labor stratification and violent crime. *Soc. Forces* 68(2):489–512.

Crutchfield RD, Geerken MR, Gove WR (1982) Crime rate and social integration: The impact of metropolitan mobility. *Criminology* 20(3–4):467–478.

Danzinger S (1976) Explaining urban crime rates. *Criminology* 14(2):291–295.

D'Arcy J, Herath T (2011) A review and analysis of deterrence theory in the IS security literature: making sense of the disparate findings. *Eur. J. Inform. Systems* 20(6):643–658.

Darley JM, Latané B (1968) Bystander intervention in emergencies: Diffusion of responsibility. 8(4, part 1):377–383.

Davenport D (2002) Anonymity on the Internet: Why the price may be too high. *Comm. ACM* 45(4):33–35.

DeHue F, Bolman C, Völlink T (2008) Cyberbullying: Youngsters' experiences and parental perception. *Cyberpsychol. Behav.* 11(2):217–223.

Delmonico DL, Griffin EJ (2008) Online sex offending: Assessment and treatment. Laws DR, O'Donohue WT, eds. *Sexual Deviance: Theory, Assessment, and Treatment* (Guilford Press, New York), 459–485.

Dooley JJ, Pyżalski J, Cross D (2009) Cyberbullying versus face-to-face bullying. *J. Psych.* 217(4):182–188.

Eagly AH, Steffen VJ (1986) Gender and aggressive behavior: A meta-analytic review of the social psychological literature. *Psych. Bull.* 100(3):309–330.

Farley S, Coyne I, Sprigg C, Axtell C, Subramanian G (2015) Exploring the impact of workplace cyberbullying on trainee doctors. *Medical Ed.* 49(4):436–443.

Freestone O, Mitchell VW (2004) Generation Y attitudes towards e-ethics and Internet-related misbehaviours. *J. Bus. Ethics* 54(2): 121–128.

Galán-García P, de la Puerta JG, Gómez CL, Santos I, Bringas PG (2016) Supervised machine learning for the detection of troll profiles in Twitter social network: Application to a real case of cyberbullying. *Logic J. IGPL* 24(1):42–53.

Garbharran A, Thatcher A (2011) Modelling social cognitive theory to explain software piracy intention. Smith M, Salvendy G, eds. *Human Interface and the Management of Information. Interacting with Information*, Lecture Notes Comput. Sci., Vol. 6771 (Springer-Verlag, Berlin Heidelberg), 301–310.

Gardner M, Steinberg L (2005) Peer influence on risk taking, risk preference, and risky decision making in adolescence and adulthood: An experimental study. *Developmental Psych.* 41(4): 625–635.

Gefen D, Rigdon EE, Straub D (2011) An update and extension to SEM guidelines for administrative and social science research. *MIS Quart.* 35(2):iii–A7.

Gibbs JP (1975) *Crime, Punishment, and Deterrence* (Elsevier, New York).

Gillespie AA (2006) Cyber-bullying and harassment of teenagers: The legal response. *J. Soc. Welfare Family Law* 28(2):123–136.

Gini G, Pozzoli T, Hymel S (2014) Moral disengagement among children and youth: A meta-analytic review of links to aggressive behavior. *Aggressive Behav.* 40(1):56–68.

Goodman JK, Cryder CE, Cheema A (2013) Data collection in a flat world: The strengths and weaknesses of Mechanical Turk samples. *J. Behavioral Decision Making* 26(3):213–224.

Hare RM (1981) *Moral Thinking: Its Method, Levels, and Point* (Oxford University Press, Oxford, UK).

Harris LC, Dumas A (2009) Online consumer misbehaviour: An application of neutralization theory. *Marketing Theory* 9(4): 379–402.

Hawdon J (2012) Applying differential association theory to online hate groups: A theoretical statement. *Res. Finnish Soc.* 5:39–47.

Hemphill SA, Heerde JA (2014) Adolescent predictors of young adult cyberbullying perpetration and victimization among Australian youth. *J. Adolescent Health* 55(4):580–587.

Higgins GE (2006) Gender differences in software piracy: The mediating roles of self-control theory and social learning theory. *J. Econom. Crime Management* 4(1):1–30.

Higgins GE, Makin DA (2004) Does social learning theory condition the effects of low self-control on college students' software piracy. *J. Econom. Crime Management* 2(2):1–22.

Higgins GE, Wolfe SE, Marcum CD (2008) Music piracy and neutralization: A preliminary trajectory analysis from short-term longitudinal data. *Internat. J. Cyber Criminology* 2(2):324–336.

Hinduja S (2007) Neutralization theory and online software piracy: An empirical analysis. *Ethics Inform. Tech.* 9(3):187–204.

Hinduja S, Patchin JW (2008) Cyberbullying: An exploratory analysis of factors related to offending and victimization. *Deviant Behav.* 29(2):129–156.

Hinduja S, Patchin JW (2010) Bullying, cyberbullying, and suicide. *Arch. Suicide Res.* 14(3):206–221.

Hinduja S, Patchin JW (2013) Social influences on cyberbullying behaviors among middle and high school students. *J. Youth Adolescence* 42(5):711–722.

Holt TJ, Burruss GW, Bossler AM (2010) Social learning and cyber-deviance: Examining the importance of a full social learning model in the virtual world. *J. Crime Justice* 33(2):31–61.

Hu Q, Xu Z, Dinev T, Ling H (2011) Does deterrence work in reducing information security policy abuse by employees? *Comm. ACM* 54(6):54–60.

Huang Y-Y, Chou C (2010) An analysis of multiple factors of cyberbullying among junior high school students in Taiwan. *Comput. Human Behav.* 26(6):1581–1590.

Jackson PI (1991) Crime, youth gangs, and urban transition: The social dislocations of postindustrial economic development. *Justice Quart.* 8(3):379–397.

Jarvis CB, MacKenzie SB, Podsakoff PM (2003) A critical review of construct indicators and measurement model misspecification in marketing and consumer research. *J. Consumer Res.* 30(2): 199–218.

Kahan DM (1997) Social influence, social meaning, and deterrence. *Virginia Law Rev.* 83(2):349–395.

Karahanna E, Straub DW, Chervany NL (1999) Information technology adoption across time: A cross-sectional comparison of pre-adoption and post-adoption beliefs. *MIS Quart.* 23(2):183–213.

Kay A (2013) At work: Cyberbullies graduate to workplace. *USA Today* (June 8). http://www.usatoday.com/story/money/columnist/kay/2013/06/08/at-work-office-cyberbullies/2398671/.

King AV (2010) Constitutionality of cyberbullying laws: Keeping the online playground safe for both teens and free speech. *Vanderbilt Law Rev.* 63(3):845–884.

Klockars CB (1974) *The Professional Fence* (Free Press, New York).

Ko CH, Yen JY, Yen CF, Chen CS, Weng CC, Chen CC (2008) The association between Internet addiction and problematic alcohol use in adolescents: The problem behavior model. *Cyberpsychol. Behav.* 11(5):571–576.

Kohlberg L (1981) *The Philosophy of Moral Development Moral Stages and the Idea of Justice* (Harper & Row, San Francisco).

Landers RN, Behrend TS (2015) An inconvenient truth: Arbitrary distinctions between organizational, Mechanical Turk, and other convenience samples. *Indust. Organ. Psych.* 8(2):142–164.

Lankton NK, Wilson EV, Mao E (2010) Antecedents and determinants of information technology habit. *Inform. Management* 47(5):300–307.

Lapidot-Lefler N, Barak A (2012) Effects of anonymity, invisibility, and lack of eye-contact on toxic online disinhibition. *Comput. Human Behav.* 28(2):434–443.

Lea M, Spears R, de Groot D (2001) Knowing me, knowing you: Anonymity effects on social identity processes within groups. *Personality Soc. Psych. Bull.* 27(5):526–537.

Lee G, Akers RL, Borg MJ (2004) Social learning and structural factors in adolescent substance use. *Western Criminology Rev.* 5(1):17–34.

Li Q (2006) Cyberbullying in schools: A research of gender differences. *School Psych. Internat.* 27(2):157–170.

Li Q (2007) New bottle but old wine: A research of cyberbullying in schools. *Comput. Human Behav.* 23(4):1777–1791.

Li Q (2008) A cross-cultural comparison of adolescents' experience related to cyberbullying. *Educational Res.* 50(3):223–234.

Limber SP (2012) *Cyberbullying: Bullying in the Digital Age* (Wiley-Blackwell, Malden, MA).

Lowry PB, Gaskin J (2014) Partial least squares (PLS) structural equation modeling (SEM) for building and testing behavioral causal theory: When to choose it and how to use it. *IEEE Trans. Professional Comm.* 57(2):123–146.

Lowry PB, Moody GD (2015) Proposing the control-reactance compliance model (CRCM) to explain opposing motivations to comply with organizational information security policies. *Inform. Systems J.* 25(5):433–463.

Lowry PB, Cao J, Everard A (2011) Privacy concerns versus desire for interpersonal awareness in driving the use of self-disclosure technologies: The case of instant messaging in two cultures. *J. Management Inform. Systems* 27(4):163–200.

Lowry PB, D'Arcy J, Hammer B, Moody GD (2016) "Cargo Cult" science in traditional organization and information systems survey research: A case for using nontraditional methods of data collection, including Mechanical Turk and online panels. *J. Strategic Inform. Systems* 25(1):232–240.

Lowry PB, Moody GD, Galletta DF, Vance A (2013) The drivers in the use of online whistle-blowing reporting systems. *J. Management Inform. Systems* 30(1):153–189.

Lowry PB, Posey C, Bennett RJ, Roberts TL (2015) Leveraging fairness and reactance theories to deter reactive computer abuse following enhanced organisational information security policies: An empirical study of the influence of counterfactual reasoning and organisational trust. *Inform. Systems J.* 25(3): 193–230.

Lowry PB, Romano NC, Jenkins JL, Guthrie RW (2009) The CMC interactivity model: How interactivity enhances communication quality and process satisfaction in lean-media groups. *J. Management Inform. Systems* 26(1):155–196.

Mangolda WG, Faulds DJ (2009) Social media: The new hybrid element of the promotion mix. *Bus. Horizons* 54(2):357–365.

Marcum CD, Higgins GE, Ricketts ML (2014) Juveniles and cyber stalking in the United States: An analysis of theoretical predictors of patterns of online perpetration. *Internat. J. Cyber Criminology* 8(1):47–56.

Markey PM (2000) Bystander intervention in computer-mediated communication. *Comput. Human Behav.* 16(2):183–188.

McFarlane L, Bocij P (2003) An exploration of predatory behaviour in cyberspace: Towards a typology of cyberstalkers. *First Monday* 8(9). http://www.firstmonday.dk/ojs/index.php/fm/article/view/1076/996.

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

Miller ME (2013) Miami student Holly Jacobs fights revenge porn. *Miami New Times* (May 9). http://www.miaminewtimes.com/2013-05-09/news/revenge-porn-miami-holly-jacobs/full/.

Minor WW (1981) Techniques of neutralization: A reconceptualization and empirical examination. *J. Res. Crime Delinquency* 18(2): 295–318.

Mitchell J, Dodder RA (1980) An examination of types of delinquency through path analysis. *J. Youth Adolescence* 9(3):239–248.

Moody GD, Siponen M (2013) Using the theory of interpersonal behavior to explain non-work-related personal use of the Internet at work. *Inform. Management* 50(6):322–335.

Moore MJ, Nakano T, Enomoto A, Suda T (2012) Anonymity and roles associated with aggressive posts in an online forum. *Comput. Human Behav.* 28(3):861–867.

Morris RG, Higgins GE (2010) Criminological theory in the digital age: The case of social learning theory and digital piracy. *J. Criminal Justice* 38(4):470–480.

Neal JW (2010) Social aggression and social position in middle childhood and early adolescence: Burning bridges or building them? *J. Early Adolescence* 30(1):122–137.

Nycyk M (2015) *Adult-to-Adult Cyberbullying: An Exploration of a Dark Side of the Internet* (Michael Nycyk, Brisbane, Australia).

Pauwels L, Schils N (2016) Differential online exposure to extremist content and political violence: Testing the relative strength of social learning and competing perspectives. *Terrorism Political Violence* 28(1):1–29.

Pershing Square Law Firm (2013) Employers must watch out for workplace cyber-bullying. Pershing Square Law Firm, Los Angeles. http://www.pershingsquarelaw.com/single-post/2013/10/15/Employers-Must-Watch-Out-for-Workplace-CyberBullying?_fb_noscript=1&href=www.pershingsquarelaw.com%2F%23!New-Law-Seeks-to-Curb-Workplace-Bullying%2Fc1tkq%2F54ff67940cf24585979af428.

Philips F, Morrissey G (2004) Cyberstalking and cyberpredators: A threat to safe sexuality on the Internet. *Convergence: Internat. J. Res. New Media Tech.* 10(1):66–79.

Pinsonneault A, Heppel N (1998) Anonymity in group support systems research: A new conceptualization, measure, and contingency framework. *J. Management Inform. Systems* 14(3):89–108.

Piotrowski C (2012) From workplace bullying to cyberbullying: The enigma of e-harassment in modern organizations. *Organ. Development J.* 30(4):44–53.

Pokin S (2007) *St. Louis Post-Dispatch*, http://www.meganmeierfoundation.org/megans-story.html.

Pornari CD, Wood J (2010) Peer and cyber aggression in secondary school students: The role of moral disengagement, hostile attribution bias, and outcome expectancies. *Aggressive Behav.* 36(2):81–94.

Posey C, Roberts TL, Lowry PB (2015) The impact of organizational commitment on insiders' motivation to protect organizational information assets. *J. Management Inform. Systems* 32(4):179–214.

Posey C, Lowry PB, Roberts TL, Ellis S (2010) Proposing the online community self-disclosure model: The case of working professionals in France and the UK who use online communities. *Eur. J. Inform. Systems* 19(2):181–195.

Posey C, Roberts TL, Lowry PB, Bennett RJ, Courtney J (2013) Insiders' protection of organizational information assets: Development of a systematics-based taxonomy and theory of diversity for protection-motivated behaviors. *MIS Quart.* 37(4): 1189–1210.

Pratt TC, Cullen FT, Sellers CS, Winfree LT Jr, Madensen TD, Daigle LE, Fearn NE, Gau JM (2010) The empirical status of social learning theory: A meta-analysis. *Justice Quart.* 27(6):765–802.

Raskauskas J, Stoltz AD (2007) Involvement in traditional and electronic bullying among adolescents. *Developmental Psych.* 43(3): 564–575.

Reicher SD, Spears R, Postmes T (1995) A social identity model of deindividuation phenomena. *Eur. Rev. Soc. Psych.* 6(1):161–198.

Renati R, Berrone C, Zanetti MA (2012) Morally disengaged and unempathic: Do cyberbullies fit these definitions? An exploratory study. *Cyberpsychol., Behav. Soc. Networking* 15(8): 391–398.

Richardson HA, Simmering MJ, Sturman MC (2009) A tale of three perspectives: Examining post hoc statistical techniques for detection and correction of common method variance. *Organ. Res. Methods* 12(4):762–800.

Ringle CM, Wende S, Will S (2005) SmartPLS 2.0 (M3) Beta. SmartPLS, Hamburg, Germany.

Robert D, Doyle J (2003) Study on cyberstalking: Understanding investigative hurdles. *FBI Law Enforcement Bull.* 72(3):10–17.

Robson C, Witenberg RT (2013) The influence of moral disengagement, morally based self-esteem, age, and gender on traditional bullying and cyberbullying. *J. School Violence* 12(2):211–231.

Rouse SV (2015) A reliability analysis of Mechanical Turk data. *Comput. Human Behav.* 43:304–307.

Sellers CS, Winfree LT (1990) Differential associations and definitions: A panel study of youthful drinking behavior. *Internat. J. Addictions* 25(7):755–771.

Siegal LJ (2011) *Criminology: The Core*, 4th ed. (Cengage Learning, Belmont, CA).

Silke A (2003) Deindividuation, anonymity, and violence: Findings from Northern Ireland. *J. Soc. Psych.* 143(4):493–499.

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

Skinner BF (1953) *Science and Human Behavior* (Macmillan, New York).

Skinner WF, Fream AM (1997) A social learning theory analysis of computer crime among college students. *J. Res. Crime Delinquency* 34(4):495–518.

Slonje R, Smith PK (2007) Cyberbullying: Another main type of bullying? *Scand. J. Psych.* 49(2):147–154.

Slonje R, Smith PK, Frisén A (2013) The nature of cyberbullying, and strategies for prevention. *Comput. Human Behav.* 29(1):26–32.

Smith PK, Mahdavi J, Carvalho M, Fisher S, Russell S, Tippett N (2008) Cyberbullying: Its nature and impact in secondary school pupils. *J. Child Psych. Psychiatry* 49(4):376–385.

Sourander A, Klomek AB, Ikonen M, Lindroos J, Luntamo T, Koskelainen M, Ristkari T, Helenius H (2010) Psychosocial risk factors associated with cyberbullying among adolescents: A population-based study. *Arch. General Psychiatry* 67(7):720–728.

Steelman ZR, Hammer BI, Limayem M (2014) Data collection in the digital age: Innovative alternatives to student samples. *MIS Quart.* 38(2):355–378.

Suler J (2004) The online disinhibition effect. *Cyberpsychol. Behav.* 7(3):321–326.

Sutherland EH (1947) *Principles of Criminology*, 4th ed. (Lippincott, Philadelphia).

Sykes GM, Matza D (1957) Techniques of neutralization: A theory of delinquency. *Amer. Sociol. Rev.* 22(6):664–670.

Tavani HT, Grodzinsky FS (2002) Cyberstalking, personal privacy, and moral responsibility. *Ethics Inform. Tech.* 4(2):123–132.

Tittle CR, Antonaccio O, Botchkovar E (2012) Social learning, reinforcement and crime: Evidence from three European cities. *Soc. Forces* 90(3):863–890.

Tokunaga RS (2010) Following you home from school: A critical review and synthesis of research on cyberbullying victimization. *Comput. Human Behav.* 26(3):277–287.

Topcu Ç, Yıldırım A, Erdur-Baker Ö (2013) Cyber bullying @ schools: What do Turkish adolescents think? *Internat. J. Advancement Counselling* 35(2):139–151.

Trumbull WN (1989) Estimations of the economic model of crime using aggregate and individual level data. *Southern Econom. J.* 56(2):423–439.

Udris R (2014) Cyberbullying among high school students in Japan: Development and validation of the online disinhibition scale. *Comput. Human Behav.* 41:253–261.

Valkenburg PM, Peter J (2011) Online communication among adolescents: An integrated model of its attraction, opportunities, and risks. *J. Adolescent Health* 48(2):121–127.

Van de Ven AH (2007) *Engaged Scholarship: A Guide for Organizational and Social Research* (Oxford University Press, New York).

Vance A, Lowry PB, Eggett DL (2015) A new approach to the problem of access policy violations: Increasing perceptions of accountability through the user interface. *MIS Quart.* 39(2): 345–366.

Vance A, Siponen M, Pahnila S (2012) Motivating IS security compliance: Insights from habit and protection motivation theory. *Inform. Management* 49(3–4):190–198.

Vandebosch H, Van Cleemput K (2009) Cyberbullying among youngsters: Profiles of bullies and victims. *New Media Soc.* 11(8): 1349–1371.

Varjas K, Talley J, Meyers J, Parris L, Cutts H (2010) High school students' perceptions of motivations for cyberbullying: An exploratory study. *Western J. Emergency Medicine* 11(3):269–273.

Venkatesh V, Thong JY, Xu X (2012) Consumer acceptance and use of information technology: Extending the unified theory of acceptance and use of technology. *MIS Quart.* 36(1):157–178.

Verrill SW (2005) Social structure and social learning in delinquency: A test of Akers' social structure-social learning model. Unpublished doctoral dissertation, University of South Florida, Tampa.

Warner BD, Pierce GL (1993) Reexamining social disorganization theory using calls to the police as a measure of crime. *Criminology* 31(4):493–517.

Winfree LT, Bäckström TV, Mays GL (1994) Social learning theory, self-reported delinquency, and youth gangs: A new twist on a general theory of crime and delinquency. *Youth Soc.* 26(2): 147–177.

Woda T (2013) Current anti-bullying and cyberbullying movements around the country. Uknowkids (March 6). http://resources.uknowkids.com/blog/bid/274139/Current-Anti-Bullying-and-Cyberbullying-Movements-Around-the-Country.

Workman M (2010) A behaviorist perspective on corporate harassment online: Validation of a theoretical model of psychological motives. *Comput. Security* 29(8):831–839.

Wright MF (2014) Predictors of anonymous cyber aggression: The role of adolescents' beliefs about anonymity, aggression, and the permanency of digital content. *Cyberpsychol., Behav., Soc. Networking* 17(7):431–438.

Xiao BS, Wong YM (2013) Cyber-bullying among university students: An empirical investigation from the social cognitive perspective. *Internat. J. Bus. Inform.* 8(1):34–69.

XpertHR (2012) Call-centre worker fairly dismissed for offensive Facebook comments about colleague. *XpertHR* (April 26). http://www.xperthr.co.uk/editors-choice/call-centre-worker-fairly-dismissed-for-offensive-facebook-comments-about-colleague/112847/.

Ybarra ML (2004) Linkages between depressive symptomatology and Internet harassment among young regular Internet users. *Cyberpsychol. Behav.* 7(2):247–257.

Ybarra ML, Mitchell KJ (2004) Youth engaging in online harassment: Associations with caregiver–child relationships, Internet use, and personal characteristics. *J. Adolescence* 27(3):319–336.