Using the Control Balance Theory to Explain Online Social Media Deviance

Paul Benjamin Lowry
The University of Hong Kong
pblowry@hku.hk

Gregory D. Moody
University of Nevada Las Vegas
greg.moody@unlv.edu

Sutirtha Chatterjee
University of Nevada, Las Vegas
sutirtha.chatterjee@unlv.edu

Abstract

Online Social Media Deviance (OSMD) is one the rise; however, research in this area traditionally has lacked a strong theoretical foundation. Following calls to reveal the theoretical underpinnings of this complex phenomenon, our study examines the causes of OSMD from several novel angles not used in the literature before, including: (1) the influence of control imbalances (CIs) on deviant behavior, (2) the role of perceived accountability and deindividuation in engendering CI, (3) and the role of IT in influencing accountability and deindividuation. Using an innovative factorial survey method that enabled us to manipulate the IT artifacts for a nuanced view, we tested our model with 507 adults and found strong support for our model. The results should thus have a strong impetus not only on future SM research but also for social media (SM) designers who can use these ideas to further develop SM networks that are safe, supportive, responsible, and constructive.

1. Introduction

Social media or SM (e.g., Facebook and Twitter) consists of "(a) the information infrastructure and tools used to produce and distribute content that has individual value but reflects shared values; (b) the content that takes the digital form of personal messages, news, ideas, that becomes cultural products; and (c) the people, organizations, and industries that produce and consume both the tools and the content" [26, p. 359]. *Online Social media deviance* (OSMD) refers to socially deviant behaviors that focus on communications enabled by SM [29]. Perhaps the most prominent online deviant acts include cyberbullying and cyberstalking, which often have serious repercussions. *Cyberbullying* has been defined as "willful and repeated harm inflicted through the medium of electronic text" [42, p. 152] with outcomes that "can be more intense, frequent, unsuspecting, and seemingly difficult to stop" [57, p. 2704]. *Cyberstalking* can be defined as "a group of behaviors in which an individual, group of individuals, or organization uses information and communication technology to harass another individual, group of individuals, or organization" [70, p. 393]. OSMD behaviors such as cyberbullying and cyberstalking have been universally termed as deviant behaviors since they cause harm to others and violate basic human rights of self-preservation [16].

SM is particularly prone to OSMD behaviors because it allows multiple privileges to users, such as posting comments on another user's page, videos, and photos and organizing groups and events. The lack of direct repercussions and the personal sense of anonymity also fosters these issues with OSMD [34]. For example, it is easier to exact revenge in a digital environment, as there are less barriers, which leads to the proliferation of OSMD [3]. Although some behaviors are relatively benign, others can be extremely damaging—such as instances of revenge porn and even extreme outcomes, such as suicide.

Given these serious issues with OSMD, researchers have recognized the need for additional research focused on the causes and prevention of OSMD [16]. Although some notable efforts have been initiated, several gaps remain, especially in designing programs to prevent such behaviors [4]. The key shortcoming of the prevention programs that have been proposed thus far is the *lack of a strong theoretical foundation* guiding their development [80]. Walker, et al. [80] summarized key issues that OSMD scholars should engage in, including the following: 1) Ensuring that OSMD phenomena are grounded in a strong theoretical base by using new and insightful theoretical perspectives; 2) Using novel research methods to address the OSMD phenomena; and 3) Engaging in causal modeling to determine the key factors associated with OSMD to better mitigate it.

Given the rapid technological advances in SM, there is not only a need to infuse a sophisticated causal theory in OSMD research but also to "consider *emerging methods and strategies* that are relevant to new and emerging media, online behaviors, and the online spaces in which young people congregate" [emphasis added] [66, pp. 197–198]. The emergence of new methods to investigate OSMD is crucial, as this area of research to date has mostly included self-reported surveys, which have their documented weaknesses [18]. Given the prior observations that technology ushers in moral issues that can perpetrate deviant behavior [8], it becomes imperative to explicitly factor in the role of technology in the theoretical and methodological investigations of OSMD to prevent OSMD.

We aim to address these opportunities in OSMD

URI: http://hdl.handle.net/10125/41427
ISBN: 978-0-9981331-0-2

research, contributing specifically in two ways. *First*, this paper offers a new theoretical perspective: the *control balance theory*, or CBT [71, 72], to investigate OSMD. This theory considers the concept of control imbalance (CI), which is particularly salient to OSMD. Given that CI between the perpetrator and the victim in OSMD has been argued to be a key factor [10], it would be useful to identify how the interplay of technology and control influence OSMD.

Recognizing the central role of CI in CBT, technology-enabled antecedents to this pivotal construct were also identified. Specifically, two fundamental *antecedents* to CI—deindividuation and perceived accountability—are significant *outcomes* of the design and implementation of IT artifacts. IT artifacts refer to the "bundles of material and cultural properties packaged in some socially recognizable form such as hardware and/or software" [41, p. 121]. We thus investigated how technology can influence perceptions of control that ultimately influence OSMD. Our key focus is how to design and manipulate IT that has a downstream effect on CI and thus to establish a strong causal theory that links technological, social, and control factors in the investigation of OSMD.

Second, this paper goes beyond the traditional experimental or survey-based approaches used in OSMD research and instead focuses on an innovative use of the factorial survey methodology (FSM) typically used in graphical user interface studies [e.g., 79]. More precisely, FSM was applied to analyze SM pages and various realistic scenarios of OSMD. This improved methodological sophistication in OSMD research allows for the examination of IT design artifacts that can cause/inhibit OSMD. Understanding the causes of OSMD has implications for improving the understanding of the phenomenon as well as understanding how to mitigate it through both IT design and laws and policies aimed at its prevention [6].

2. Control Balance Theory (CBT)

CBT [71, 72], a criminological theory, is an important lens to explain the OSMD phenomenon. CBT introduces the key concept of control, which is fundamental to OSMD but noticeably absent in extant OSMD research [17]. Specifically, one key issue in OSMD research is *CI*, which is caused by the negative power differential between the victim and the OSMD perpetrator [51, 55]. Much of the nascent research on OSMD concludes that such activities arise from a power differential between the attacker and the victim [13]. Others concur, arguing that:

… [OSMD] is centered on the systematic abuse of power and control over another individual who is perceived to be vulnerable and weaker…" [37, p. 323].

Notably, because the power imbalance is repeatedly abused in a systemic manner in OSMD [64], CBT is appropriate for investigating this phenomenon. In CBT, *deviance* is defined as "any behavior that the majority of a given group regards as unacceptable or that typically evokes a collective response of a negative type" [71, p. 124]. Hence, OSMD fits nicely in this conceptualization of deviance.

The basic concept of CBT is that "the amount of control to which an individual is subject, relative to the amount of control he or she can exercise, determines the probability of deviance occurring as well as the type of deviance likely to occur" [71, p. 135]. This is illustrated by the concept of the control balance (CB) ratio (CBR), which is the ratio between the amount of control exerted upon others and the exposure to control on the individual by others. Generally, deviance increases with CBRs that depart from a balance control ratio of 1 (capturing imbalance). Conversely, as the control ratio arrives nearer to a balanced ratio (i.e., 1), deviance also decreases. CBT further proposes that people react in a deviant manner because they perceive or experience a CI with respect to their victims [71].

CBT is useful and generalizable, as noted in [45], because it is designed to explain "all forms of deviance committed by all types of deviant actors" (p. 324). Criminological researchers have argued that it is "more nuanced and elaborate than previous control theories" [14, p. 271]; however, CBT has not particularly been applied to computer-dependent behaviors, such as OSMD [22]. Recognizing this gap, we aim to be among the first to implement CBT to investigate OSMD and contend that it would be a useful contribution to OSMD scholarship.

Although CI (defined by the CBR deviating from a value of 1) is perhaps the most important tenet of CBT, academic work on CBT has consistently argued the salience of another factor, namely *moral beliefs*, because this construct offers a counterpoint to the enactment of deviance, even in the face of CI. In the words of Paternoster and Simpson [43, p. 44-45]: "Those with strong moral inhibitions are predicted to refrain from committing a particular offense **no matter what**" [Emphasis added]. Notably, Tittle, et al. [73] also asserted that moral beliefs are often considered the central tenet of theories investigating social behavior, thus making them salient to any investigation of criminological behavior, such as deviant acts. Empirically, research has consistently demonstrated that moral beliefs have a negative and *independent* impact on deviance [2]. Thus, moral beliefs are significant deterrents to deviant acts [8], thereby justifying their inclusion in our model.

Whereas CBT highlights the central construct of CI and how it affects OSMD, it is unknown how CI itself is linked with other constructs, especially in a technological context, such as SM. Accordingly, we introduce two key concepts that are arguably pivotal

antecedents to CI and that are influenced by technological design and features. These two salient concepts are *deindividuation* and *perceived accountability*.

Deindividuation can be defined as a "decrease in self-observation, self-evaluation, and concern for social comparison and evaluation" [9, p. 3044]. There are two reasons that deindividuation becomes central in this context. First, deindividuation has been consistently associated with deviant behavior [83]. Second, deindividuation is quite rampant in virtual environments, including SM [21]. Specifically, it has been argued that the virtual environment creates deindividuation effects that ultimately engender deviant behavior [12], including online harassment, which is a type of OSMD [24]. It is thus natural to infer that deindividuation has a strong link with CI.

The next construct that is an antecedent to CI is *perceived accountability*. This is defined as the perceptions of "the implicit or explicit pressure to justify one's beliefs and actions to others" [69, p. 8]. Recent research has stressed the importance of accountability in virtual environments [79] and has also highlighted that perceptions of accountability are often lowered in virtual environments [81]. In fact, as accountability increases, demands on ethical behavior become more prominent, leading to more conformist and less deviant behaviors [23]. Thus, if accountability leads to less deviant behaviors and CI leads to more deviant behaviors, a negative relationship could exist between accountability and CI.

Having proposed the two important antecedents of CI, this question naturally arises: What role does IT have in engendering these antecedents? There is sufficient evidence that technology design and features can influence deviant behavior [8]. Thus, there is a need to understand which IT design features affect the key constructs of deindividuation and perceived accountability. Recent IS research summarizes *four fundamental characteristics* of IT design artifacts that are arguably crucial, including IT design features that promote social anonymity, monitoring awareness, evaluation awareness, and social presence awareness [78, 79]. Arguably, the ability to implement such IT design features has strong implications for deindividuation and perceived accountability, which causes it to be salient in the central concept of CI. This extended theoretical framework is discussed in the hypotheses development section.

3. Hypotheses Development

3.1 Control Imbalance (CI)

According to CBT, individuals engage in deviant behavior if they experience a CI, which is a CBR that deviates from 1 [72]. This imbalance is often perceived as an opportunity to improve their CBR (either because the CBR <1, which they want to rectify, or because the CBR>1, which they want to leverage). That is, deviant behavior results from an attempt to "escape deficits [CBR<1] and extend surpluses [CBR>1] of control." An individual who is aware of the imbalance of his or her control ratio becomes more motivated to engage in deviant behaviors.

CI becomes particularly salient in SM environments. Compared to physical interactions, SM, such as Facebook, can be more easily misappropriated for deviant purposes due to their ubiquity and proliferation and the low barrier to entry [40]. Indeed, there is an emergent consensus that social networks support deviant behavior because they allow deviant behavior to spread quickly [39]. Interactions via SM can allow individuals to engage with distant and remote acquaintances [44] whom they feel much less connected to and consequently perceive greater control to engage in deviant acts. One subject of the [44, p. 235] study commented on the voyeuristic nature of Facebook:

"Facebook is extremely voyeuristic – there's something great, and at the same time, creepy, about knowing when someone you haven't talked to in 5 years broke up with their boyfriend who you never even met"

The voyeuristic capabilities of SM sites allow individuals to know intimate details about others, which means that they may know more about their weaknesses and thus perceive greater control in harming them. Although this creates one form of CI, SM can create CIs in the opposite manner. For example, individuals could also learn about the positive experiences of others through the voyeuristic means afforded by SM, which may excite jealousy (due to the perceived differential) and defiance [46], leading to intentions to harm others through the platform of SM. In summary, CI creates a motivation to act in a deviant manner. Thus:

H1. CI positively influences OSMD.

3.2 Moral Beliefs

Deviant behavior is inherently unethical, as it is contradictory to prevailing ethical norms. It has been consistently established in prior research that moral beliefs play a strong role in deterring unethical behavior, including in the use of IT. According to prior research, moral beliefs can be understood to be an "informal sanction variable" and "self-imposed punishment can be an inhibiting factor" [25, p. 100].

Moral beliefs "stem from concepts of welfare, justice, and rights'' [75, p. 170]. Individuals often use their moral beliefs to judge whether an act is justifiable and ethical [33]. It has been argued that individuals who engage moral beliefs are able to empathize with others (possible victims of their actions) and as a result, feel negative affective reactions when contemplating deviant acts, including those on the internet or SM [7].

Thus, moral beliefs are strongly predictive of any unethical/deviant behavior, albeit in a negative manner. Literature also consistently shows that moral beliefs mostly have an independent effect while influencing deviant behavior (as an aside, we later empirically tested for moderating effects of moral beliefs which were absent). This is true even if the behavior is enacted via SM since moral beliefs that view OSMD as a moral violation are likely to refrain from doing so [27]. Hence, "the higher one's moral beliefs, the less likely an individual is to intend to engage in the deviant act" [59, p. 54]. Thus:

H2. Moral beliefs negatively influence OSMD.

3.3 Deindividuation

Deindividuation has a strong influence on how people perceive the concept of CI. Due to the reduced connection to the social context as a result of deindividuation, individuals feel less of a possibility of sanctions and constraints that can result from any deviant behavior [50]. Notably, individuals in a virtual mode (as in SM contexts) "are less receptive to sanction threats pertaining to the improper use of IS resources" [11, p. 647].

When individuals are deindividuated, they lose their sense of shame or guilt and often perceive that they are in greater control of their deviant behaviors (or intentions). This creates a CI. Their ability to express their innermost desires, while hiding behind the mediation of cyberspace, provides ample opportunities to engage in deviant behavior. Interacting with computers in general leads individuals feeling "released to behave badly" due to the reduced probability of constraints interfering with their deviant action [82].

Moreover, individuals are less self-critical in deindividuated contexts [61], which makes them seemingly more in control. For example, research has shown that even when individuals face informal sanctions, such as public shaming, they become averse to committing deviant behaviors [53]. In deindividuated contexts of temporal and spatial separation coupled with the possibility of a hidden identity (such as by using pseudonyms or fake identities), the opposite occurs. Individuals then become more confident that they can engage in deviant behaviors (i.e., can control what they do to others) as compared to facing sanctions for them (i.e., how others can control them). Thus, deindividuation leads to an increase in CI by increasing the control exerted, while decreasing the control experienced for OSMD behaviors. Hence:

H3. Deindividuation positively affects CI for OSMD.

3.4 Accountability and OSMD

As noted in [79], one of the important effects of perceived accountability is an increase in conservatism, especially when negative behaviors are considered. Many studies have argued that individuals with heightened perceptions of conservatism essentially perceive that while they may have the power to commit certain deviant acts, others can also sanction those acts [36]. A classic example is an organizational/community leader who wields power over others, but this very power also places leaders in the cynosure of others, which increases the possibility of sanction should they commit any deviant act. Accordingly, an individual who perceives that s/he may have the wherewithal to commit a deviant act (due to a position of power) but is also accountable due to this very wherewithal perceives their power and control as neutralized [20], which restores CB.

Regarding the relation between perceived accountability and CI, our argument can be summarized as follows. To increase their CBR, individuals often use justificatory rationalizations to reduce their possible sense of guilt and shame for deviant behavior [cf., 63]; however, accountability acts as an opposition to this process and balances this increased CBR. Furthermore, in a SM environment that allows the perpetrator to wield control over the victim, accountability neutralizes this control surplus by the perception that any deviant behavior will be sanctioned [48] by being discovered [56]. To conclude, perceived accountability in a SM environment arguably maintains CB. That is, it prevents CIs from occurring, and thus, logically, it negatively influences CI. Thus,

H4. Accountability negatively affects CI for OSMD.

3.5 Influence of IT Design Features on Deindividuation and Accountability: Positive Effects

3.5.1 Social Anonymity and Deindividuation

In a SM context, if users are not identifiable (i.e., anonymous), then a state of deindividuation occurs [61]. This is why OSMD perpetrators experience less self-awareness, self-evaluation, and self-comparison; they can *hide* behind the Internet medium [61]. This is a classic case of deindividuation, which ultimately promotes deviant behavior that is often irrational, impulsive, and aggressive [37]. If perpetrators of OSMD can be potentially identifiable, then the opposite occurs in which individuals are more alert, critical, and apprehensive of the outcomes of their deviant behavior.

H5a. Anonymity positively affects deindividuation.

3.5.2 Social Presence Awareness and Accountability

Social presence awareness can be defined as "the degree by which a person was perceived as 'real'" [30, p. 297] and the level to which they are perceived to react to an actor [62]. Social presence awareness incorporates both knowledge of social ties as well as social emotions [32]. In the context of SM, it has been argued that SM features may also facilitate social presence awareness [54]. When individuals experience a heightened social presence through technological

interactions, they are forced to cognitively and systematically process the effect of their behavior on others, thus increasing accountability [79]. Thus:

H5b. Social presence positively affects accountability.

3.5.3 Monitoring Awareness and Accountability

Monitoring awareness is the consciousness that one's activities are being tracked and watched [79]. It becomes important in the context of social networks, as they afford monitoring in a socially acceptable manner [76]. Social networks can have monitoring mechanisms built in through which user behaviors can be tracked and unacceptable behaviors can be punished [67].

If SM is developed with technological controls that increase individual's perceptions of monitoring awareness, they will likely heighten the possible accountability for a person's acts on SM. For example, if users are aware that the SM interface can be used to monitor their actions, they will feel that they may be held accountable for their actions at a later point in time. This is especially true for OSMD because accountability perceptions should become more salient in contexts in which there is possibility of sanctions and future repercussions. Thus, we predict:

H5c. Monitoring positively affects accountability.

3.5.4 Evaluation and Accountability

Although the perception that one is being monitored is salient to SM behavior, the perceptions that those monitored actions will be evaluated for determining potential consequences adds another degree of accountability to user behaviors [31]. *Evaluation awareness* refers to the users' knowledge that their actions are being logged as well as reviewed [74]. In general, perceptions of evaluation awareness tend to make people engage less in unacceptable behaviors [1]. Researchers have argued that as people become more aware that their actions are being evaluated, they behave in a more acceptable fashion, while also reducing their unacceptable behavior as accountability perceptions are heightened [74, 78, 79]. Thus:

H5d. Evaluation positively affects accountability.

3.6 Influence of IT Design Features on Deindividuation and Accountability: Negative Effects

3.6.1 Social Anonymity and Accountability

Social anonymity is defined as the degree to which others have knowledge of a person's online interactions [34]. In technological systems, IT artifacts can be designed to affect anonymity [34]. Because accountability can be understood as "being answerable to audiences for performing up to certain prescribed standards, thereby fulfilling obligations, duties, expectations, and other charges" [58, p. 634], when an individual cannot be identified, s/he becomes less accountable for any action perpetrated by him/her.

By definition, a crime (i.e., deviant behavior) should be identifiable, being defined as "any *identifiable* behavior that an appreciable number of governments has specifically prohibited and formally punished" [19, p. 35]; thus, making the perpetrator unidentifiable contributes to reduced accountability [65]. Thus:

H6a. Anonymity negatively affects accountability.

3.6.2 Social Presence and Deindividuation

IT interfaces rich in social presence allow for effective as well as broader information transfer (e.g., sharing profiles on SM) [28]. In fact, it has been argued that the increased social presence improves information exchange in a social network [5]. This creates greater awareness of others in a virtual context, which is arguably due to increased "cognition and systematic processing" about others [79]. This heightened awareness is contradictory to deindividuation in online environments. Deindividuation is synonymous with reduced awareness, whether of oneself or of others [15]. It implies the inability to monitor, control, and plan behavior [49] and being impulsive, irrational, and emotional [83]. It is thus clear that technological features that promote social presence awareness, bring people together, encourage knowledge-sharing, and make users aware and contemplative of others have a negative effect on deindividuation. Thus:

H6b. Social presence negatively affects deindividuation.

4. Design and Methodology

4.1 Factorial Survey Design and Manipulations

As explained in [79], the factorial survey method (FSM) has effective, unique properties that allow it to leverage the strengths of both surveys and experiments, and it allows for the testing of a large number of manipulations without suffering from otherwise expected multicollinearity problems. By combining huge numbers of combinations along with vignettes that have contextual details, this method has the benefit of providing experimental control but with a level of realism in the ethical and decision-making details, which is simply not possible to accomplish under any other method [79].

Our FSM design consisted of the following: 2 (high vs. low social anonymity conditions) x 2 (high vs. low monitored conditions) x 2 (high vs. low evaluation expectation conditions) x 2 (known social network—Facebook vs. unknown social network—VK) x 3 (highly vs. moderately vs. low risk to OSMD). These manipulations were delivered through a combination of textual and graphical treatments. The subjects were randomly assigned to a treatment condition by the online survey engine. The inclusion of risk as a condition was necessitated because cyberbullying behaviors can range from relatively benign to criminal,

thus inherently adding the severity of sanctions associated with the risk of being caught as an important consideration. (See Appendix C in this link for example behaviors within the scenarios). Following [79], we used a combination of graphical and textual treatments with hypothetical OSMD vignettes to fully maximize the use of the factorial survey method. See Appendix B in this link for examples. Details of the procedures can also be found in this link.

4.2 Data Collection via Mechanical Turk

The majority of constructs were measured by multiple indicators using seven-point Likert-type scales adapted from existing literature [e.g., 79] (see Appendix A in this link); however, CI was measured by the ratio of control exerted to the control subjected. Because our focus in our theory development was on CI and how it was influenced (irrespective of whether it is control surplus or control deficit), any value of the control ratio less than 1 (indicating a control deficit) was inverted (1/x) so that the CI measure was always greater than one and the CI increased in a unidirectional manner. Due to space constraints all details regarding the empirical study, including procedures, instrument development, pilot testing, and final analysis are presented in the online appendix in this link.

Following three pilot studies, for the final data collection, we used the setup from the third pilot test (which required no further improvements), and recruited 652 participants by means of Amazon's Mechanical Turk™ [e.g., 60]. Experimental results from participants recruited on Mechanical Turk are comparable with those of lab experiments or online experiments with student participants, while obtaining the results is comparatively fast and inexpensive [38]. The incentive for participating in this study was US$3, which is on the higher side of compensation for Mechanical Turk. We also followed some additional guidelines for preventing common-method bias and improving data quality in online panel studies, per [34, 35], creating a final usable sample size of 507. Moreover, we gathered a marker variable (i.e., resentment) so that we could use the marker-variable technique to test for mono-method bias ex post facto [47]. The sample demographics are available in this link.

5. Analyses

Manipulation checks using mean differences and MANOVA techniques indicated that our manipulations were significant ($p<0.0001$). Following that, we used the covariance-based SEM (CB-SEM) tool, STATA (version STATA/SE 14.0), for our analysis. The model fit was good: $\chi^2_{310} = 997.543$; $\chi^2/df = 3.22$; CFI= 0.943; TLI = 0.935; RMSEA = 0.068; SRMR = 0.074; CD = 1.000. The convergent validity was supported by large and standardized loadings for all constructs ($p < .001$) and *t*-values that exceeded statistical significance. Convergent validity was also supported by calculating the ratio of factor loadings to their respective standard errors that exceed |10.0| ($p < .001$) (see Appendix C in this link).

Discriminant validity was tested by showing that the measurement model had a significantly better model fit than a competing model with a single latent construct and was better than all other competing models in which pairs of latent constructs were joined. To test for common-method bias, a marker variable (resentment) was entered into the model. It was not significant on our intention variable, indicating that a method bias is not likely present in our data. Finally we tested for mediation tests using procedures noted in the literature [e.g., 79]. These additional analyses further support our model and are carefully detailed in Online Appendix C in this link.

6. Discussion of Results

All hypotheses in our model were strongly supported (see Figure 1). Our results provide the following salient insights into the OSMD phenomenon: 1) CI is a key facilitator of OSMD; 2) Moral beliefs are strong inhibiting factors in OSMD; and 3) Key IT design artifacts of the virtual environment create powerful downstream effects on CIs. It is clear from our investigation that OSMD arises in a situation of CI between the perpetrator and the victim. This finding is quite consistent with the existing views that SM are breeding grounds for CI, being "…spheres of…hegemony (power),…leading to greater fragmentation of social relations…" [52, p. 161].

Recognizing this often dysfunctional nature of SM environments, researchers are beginning to question whether such environments inhibit relationships and cause distractions, thereby leading to social disengagement. Others have pointed out that SM provides a breeding ground for narcissism in which the focus is making oneself popular and attractive and thus inherently more powerful [77]. In other situations, SM relationship endings are often not mutual: one can be "unfriended" without immediately realizing it. For example, relationship dissolution via SM (e.g., unfriending or blocking) is a key example of CI that gives the perpetrator unilaterally more control of the relationship. Conversely, such imbalances and their deviant outcomes create further imbalance and further deviant outcomes when the negative emotions felt by the victims (e.g., jealousy or other emotional devastation) are released on SM. It is important to note here that "unfriending" is not necessarily a dysfunctional act; however, it can breed dysfunctional retaliations.

Second, another key finding is that moral beliefs are

strong OSMD deterrents. Moral beliefs are often conceived as informal sanctions that factor in disapproval (for an action) by both oneself and others. This is consistent with prior research, which views moral beliefs as playing a role on self-imposed punishment of deviant behavior (ibid), one that has been empirically supported in multiple studies that argue that higher moral beliefs tend to negatively influence deviant intention.

Since moral beliefs are often formed during primary and secondary socialization [8], it may be difficult to modify them in adulthood. What is more feasible in an immediate context is to design IT artifacts that can dissipate CI, thereby leading to more conformist and less deviant behaviors. In this regard, our study shows that IT design artifacts can promote better CB downstream and thus mitigate OSMD, regardless of moral beliefs. This finding has crucial implications, especially in light of the negative repercussions of technology in OSMD, because it has been argued that technology plays a supporting role in OSMD.

There are many challenges created by IT in a SM context, and all contribute in some way to the power/CI that ultimately fosters deviant behavior. Sugarman and Willoughby [68] enumerated technological features that inherently enable power imbalance from different aspects, ranging from anonymity to advanced technological skills, as well as an avenue for retaliation to offline misbehavior. In summary, the IT mediated environment provides a way to control others, provides a way for one to feel controlled by others, and supports ways to retaliate in offline control, which indicates that the SM environment is a haven for CI. Thus, the four IT artifact design features in our study, social anonymity, social presence, evaluation awareness, and monitoring awareness, acquire greater criticality in this regard, because ultimately, it is these IT design features that influence OSMD downstream. For example, explicitly building in features that can monitor an individual's cyber-behavior (e.g. the pages that one visits) would make potential perpetrators wary of committing OSMD, as they would feel more accountable to behave responsibly. Knowing this, we can accordingly design IT (as per these features) to thwart CI and ultimately prevent OSMD.

6.1 Contributions to Research and Practice

We are among the first to introduce CBT, particularly using the constructs of control surplus and control deficit, into the context of OSMD. Both control surplus (i.e., one feels he/she is in control of others) and control deficit (i.e., one feels he/she is controlled by others) are destabilizing factors that are related to increased OSMD intention. CBT introduces the key concepts of power and control and deals with power imbalances that are abused systematically, which are fundamental to OSMD but generally missing in the other theoretical accounts of OSMD. As explained by CBT, CIs increase one's intention to engage in OSMD, as supported in this study. We also show that the abundance or lack of power is pivotal. In several of our scenarios, the victim attacks back, feeling powerless, but retaliations also occur from those who experience greater power over their victims. We found further support that CBR is influenced by two antecedents: deindividuation and perceived accountability. Such findings illuminate the nomological network of CBR in leading to a better understanding of this phenomenon.

We also are among the first to apply the accountability theory in the OSMD literature. This is particularly important because we emphasize IT artifacts design features that have not been considered in this literature: monitoring awareness, evaluation awareness, social presence, and an expanded conceptualization of social anonymity. We demonstrate how through accountability design and decreased CIs, the IT artifact design features can be leveraged to decrease OSMD. We note that in designing our treatments for this study, we focused on elements that already existed in the current social networking platforms and were not investigating new elements or interventions that could potentially further improve perceived accountability or decrease deindividuation.

6.2 Future Research and Conclusion

To challenge our model, we tested a number of control variables that may act as counter explanations to what predicts OSMD. Several of these were significant but were not too surprising, as they followed patterns seen in the literature: informal risk (-), education (+), computer experience (-), computer proficiency (+), SM experience (-), and cyberstalking habit (+); yet, there control results that should be explored in future research. For example, whereas computer experience was a negative predictor, computer proficiency and education were positive predictors. Researchers should consider similar negative indicators in future studies.

To conclude, we hope that this study provides a strong theoretical foundation for OSMD research, and identifies IT-related factors that future OSMD research could look into. We feel that design of IT features that could prevent OSMD should be an especially fruitful line of inquiry. We urge future research to actively engage in this endeavor so as to combat the growing problem of OSMD.

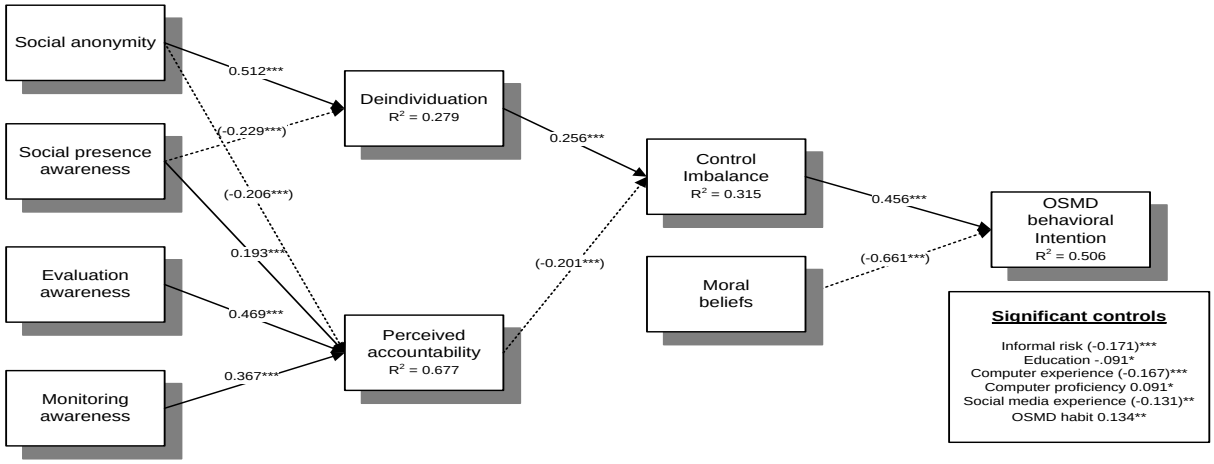

Figure 1. Structural Model Results

References

[1] Adler, A.; Nash, J.C.; and Noël, S. Evaluating and implementing a collaborative office document system. *Interacting with computers*, 18, 4 (2006), 665-682.

[2] Baron, S.W. Street youths' control imbalance and soft and hard drug use. *Journal of Criminal Justice*, 38, 5 (2010), 903-912.

[3] Bauman, S.; Cross, D.; and Walker, J. *Principles of cyberbullying research: Definitions, measures, and methodology*. New York, NY: Routledge, 2013.

[4] Bauman, S. and Yoon, J. This issue: Theories of bullying and cyberbullying. *Theory Into Practice*, 53, 4 (2014), 253-256.

[5] Beck, R.; Pahlke, I.; and Seebach, C. Knowledge exchange and symbolic action in social media-enabled electronic networks of practice: A multilevel perspective on knowledge seekers and contributors. *Management Information Systems Quarterly*, 38, 4 (2014), 1245-1270.

[6] Campbell, M.A. How research findings can inform legislation and school policy on cyberbullying. In S. Bauman, D. Cross, and J. Walker (eds.), *Principles of cyberbullying research, definitions, measures, and methodology*. New York, NY: Routledge, 2013, pp. 290-303.

[7] Campbell, M.A.; Slee, P.T.; Spears, B.; Butler, D.; and Kift, S. Do cyberbullies suffer too? Cyberbullies' perceptions of the harm they cause to others and to their own mental health. *School Psychology International*, 34, 6 (2013), 613-629.

[8] Chatterjee, S.; Sarker, S.; and Valacich, J.S. The behavioral roots of is security: Exploring key factors of unethical it use. *Journal of Management Information Systems*, 31, 4 (2015), 49-87.

[9] Christopherson, K.M. The positive and negative implications of anonymity in internet social interactions:"On the internet, nobody knows you're a dog". *Computers in Human Behavior*, 23, 6 (2007), 3038-3056.

[10] Cross, D.; Bauman, S.; and Walker, J. Summary and conclusions. In D. Cross, S. Bauman, and J. Walker (eds.), *Principles of cyberbullying research: Definitions, measures, and methodology*. New York, NY: Routledge, 2013, pp. 337-353.

[11] D'Arcy, J. and Herath, T. A review and analysis of deterrence theory in the is security literature: Making sense of the disparate findings. *European Journal of Information Systems*, 20, 6 (2011), 643-658.

[12] D'Arcy, J. and Hovav, A. Does one size fit all? Examining the differential effects of is security countermeasures. *Journal of Business Ethics*, 89, 1 (2009), 59-71.

[13] Davison, C.B. and Stein, C.H. The dangers of cyberbullying. *North American Journal of Psychology*, 16, 3 (2014), 595-606.

[14] DeLisi, M. and Hochstetler, A. An exploratory assessment of tittle's control balance theory: Results from the national youth survey. *The Justice Professional*, 15, 3 (2002), 261-272.

[15] Diener, E. Deindividuation, self-awareness, and disinhibition. *Journal of Personality and Social Psychology*, 37, 7 (1979), 1160.

[16] Dinakar, K.; Jones, B.; Havasi, C.; Lieberman, H.; and Picard, R. Common sense reasoning for detection, prevention, and mitigation of cyberbullying. *ACM Transactions on Interactive Intelligent Systems (TiiS)*, 2, 3 (2012), 18.

[17] Espelage, D.L.; Rao, M.A.; and Craven, R.G. Theories of cyberbullying. In S. Bauman (ed.), *Principles of cyberbullying research: Definitions, measures, and methodology*. New York, NY: Routledge, 2013, pp. 78-97.

[18] Espinoza, G. and Juvonen, J. Methods used in cyberbullying research. In S. Bauman, D. Cross, and J. Walker (eds.), *Principles of cyberbullying research, definitions, measures, and methodology*. New York, NY: Routledge, 2013, pp. 142-154.

[19] Felson, M. *Gime and nature*. Thousand Oaks, CA: Sage Publications, 2006.

[20] Fiske, S.T. Controlling other people: The impact of power on stereotyping. *American Psychologist*, 48, 6 (1993), 621-628.

[21] Fox, J. and Tang, W.Y. Sexism in online video games: The role of conformity to masculine norms and social dominance orientation. *Computers in Human Behavior*, 33, (2014), 314-320.

[22] Fox, K.A.; Nobles, M.R.; and Fisher, B.S. A multi-theoretical framework to assess gendered stalking victimization: The utility of self-control, social learning, and control balance theories. *Justice Quarterly*, (2014), 1-29.

[23] Hall, A.T.; Frink, D.D.; and Buckley, M.R. An accountability account: A review and synthesis of the theoretical and empirical research on felt accountability (in press). *Journal of Organizational Behavior*, forthcoming, (2015),

[24] Halpern, D. and Gibbs, J. Social media as a catalyst for online deliberation? Exploring the affordances of facebook and youtube for political expression. *Computers in Human Behavior*, 29, 3 (2013), 1159-1168.

[25] Hovav, A. and D'Arcy, J. Applying an extended model of deterrence across cultures: An investigation of information systems misuse in the u.S. And south korea. *Information & Management*, 49, 2 (2012), 99-110.

[26] Howard, P.N. and Parks, M.R. Social media and political change: Capacity, constraint, and consequence. *Journal of communication*, 62, 2 (2012), 359-362.

[27] Jiang, Z.; Heng, C.S.; and Choi, B.C. Research note—privacy concerns and privacy-protective behavior in synchronous online social interactions. *Information Systems Research*, 24, 3 (2013), 579-595.

[28] Kane, G.C.; Alavi, M.; Labianca, G.; and Borgatti, S.P. What's different about social media networks? A framework and research agenda. *MIS Quarterly*, 38, 1 (2014), 275-304.

[29] Kowalski, R.M.; Limber, S.; Limber, S.P.; and Agatston, P.W. *Cyberbullying: Bullying in the digital age*. Malden, MA Wiley/Blackwell, 2012.

[30] Lambropoulos, N.; Faulkner, X.; and Culwin, F. Supporting social awareness in collaborative e-learning. *British Journal of Educational Technology*, 43, 2 (2012), 295-306.

[31] Lee, J.; Crossler, R.; and Warkentin, M. Implications of monitoring mechanisms on bring your own device (byod) adoption. (2013),

[32] Liechti, O. and Ichikawa, T. A digital photography framework supporting social interaction and affective awareness. In G. Goos, J. Hartmanis, and J.v. Leeuwen (eds.), *Handheld and ubiquitous computing*. Berlin Heidelberg: Springer, 1999, pp. 186-192.

[33] Liu, Z.; Yang, Z.; Zeng, F.; and Waller, D. The developmental process of unethical consumer behavior: An investigation grounded in china. *Journal of Business Ethics*, 128, 2 (2015), 411-432.

[34] Lowry, P.B.; Moody, G.D.; Galletta, D.F.; and Vance, A. The drivers in the use of online whistle-blowing reporting systems. *Journal of Management Information Systems*, 30, 1 (2013), 153-190.

[35] Lowry, P.B.; Posey, C.; Bennett, R.J.; and Roberts, T.L. 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. *Information Systems Journal*, 25, 3 (2015), 193–230.

[36] Maner, J.K.; Gailliot, M.T.; Butz, D.A.; and Peruche, B.M. Power, risk, and the status quo: Does power promote riskier or more conservative decision making? *Personality and Social Psychology Bulletin*, 33, 4 (2007), 451-462.

[37] Mason, K.L. Cyberbullying: A preliminary assessment for school personnel. *Psychology in the Schools*, 45, 4 (2008), 323-348.

[38] Mason, W. and Suri, S. Conducting behavioral research on amazon's mechanical turk. *Behavior Research Methods*, 44, 1 (2012), 1-23.

[39] McCuddy, T. and Vogel, M. Beyond traditional interaction: Exploring the functional form of the exposure-offending association across online network size. *Journal of Criminal Justice*, 43, 2 (2015), 89-98.

[40] Nobles, M.R.; Reyns, B.W.; Fox, K.A.; and Fisher, B.S. Protection against pursuit: A conceptual and empirical comparison of cyberstalking and stalking victimization among a national sample. *Justice Quarterly*, 31, 6 (2012), 986-1014.

[41] Orlikowski, W.J. and Iacono, C.S. Research commentary: Desperately seeking the "it" in it research—a call to theorizing the it artifact. *Information systems research*, 12, 2 (2001), 121-134.

[42] Patchin, J.W. and Hinduja, S. Bullies move beyond the schoolyard a preliminary look at cyberbullying. *Youth violence and juvenile justice*, 4, 2 (2006), 148-169.

[43] Paternoster, R. and Simpson, S. A rational choice theory of corporate crime. In R. Clarke, and M. Felsoncrime (eds.), *Advances in criminological theory: Routine activity and rational choice*. New Brunswick, NJ: Transaction, 1993, pp. 37-58.

[44] Pempek, T.A.; Yermolayeva, Y.A.; and Calvert, S.L. College students' social networking experiences on facebook. *Journal of Applied Developmental Psychology*, 30, 3 (2009), 227-238.

[45] Piquero, A.R.; MacIntosh, R.; and Hickman, M. Applying rasch modeling to the validity of a control balance scale. *Journal of Criminal Justice*, 29, 6 (2001), 493-505.

[46] Piquero, N.L. and Piquero, A.R. Control balance and exploitative corporate crime. *Criminology*, 44, 2 (2006), 397.

[47] Podsakoff, P.M.; MacKenzie, S.B.; Lee, J.Y.; and Podsakoff, N.P. Common method biases in behavioral research: A critical review of the literature and recommended remedies. *Journal of Applied Psychology*, 88, 5 (2003), 879-903.

[48] Pogarsky, G. and Piquero, A.R. Studying the reach of deterrence: Can deterrence theory help explain police misconduct? *Journal of Criminal Justice*, 32, 4 (2004), 371-386.

[49] Postmes, T. and Spears, R. Deindividuation and antinormative behavior: A meta-analysis. *Psychological Bulletin*, 123, 3 (1998), 238-259.

[50] Postmes, T.; Spears, R.; and Lea, M. Breaching or building social boundaries? Side-effects of computer-mediated communication. *Communication research*, 25, 6 (1998), 689-715.

[51] Privitera, C. and Campbell, M.A. Cyberbullying: The new face of workplace bullying? *CyberPsychology & Behavior*, 12, 4 (2009), 395-400.

[52] Rahimi, B. The agonistic social media: Cyberspace in the formation of dissent and consolidation of state power in postelection iran. *Communication Review*, 14, 3 (2011), 158-178.

[53] Rebellon, C.J.; Piquero, N.L.; Piquero, A.R.; and Tibbetts, S.G. Anticipated shaming and criminal offending. *Journal of Criminal Justice*, 38, 5 (2010), 988-997.

[54] Riedl, C.; Köbler, F.; Goswami, S.; and Krcmar, H. Tweeting to feel connected: A model for social connectedness in online social networks. *International Journal of Human-Computer Interaction*, 29, 10 (2013), 670-687.

[55] Rivituso, J. Cyberbullying victimization among college students: An interpretive phenomenological analysis. *Journal of Information Systems Education*, 25, 1 (2014), 71-75.

[56] Rothe, D.L. and Mullins, C.W. Toward a criminology of international criminal law: An integrated theory of international criminal violations. *International Journal of Comparative and Applied Criminal Justice*, 33, 1 (2009), 97-118.

[57] Sabella, R.A.; Patchin, J.W.; and Hinduja, S. Cyberbullying myths and realities. *Computers in Human Behavior*, 29, 6 (2013), 2703-2711.

[58] Schlenker, B.R.; Britt, T.W.; Pennington, J.; Murphy, R.; and Doherty, K. The triangle model of responsibility. *Psychological review*, 101, 4 (1994), 632-652.

[59] Schoepfer, A. and Piquero, A.R. Self-control, moral beliefs, and criminal activity. *Deviant Behavior*, 27, 1 (2006), 51-71.

[60] Schulze, T.; Krug, S.; and Schader, M. Workers' task choice in crowdsourcing and human computation markets. Presented at *ICIS 2012*, Orlando, FL, 2012.

[61] Scott, S.V. and Orlikowski, W.J. Entanglements in practice: Performing anonymity through social media. *MIS Quarterly*, 38, 3 (2014), 873-893.

[62] Shen, K.N. and Khalifa, M. Design for social presence in online communities: A multidimensional approach. (2009),

[63] Siponen, M. and Vance, A. Neutralization: New insights into the problem of employee systems security policy violations. *MIS Quarterly*, 34, 3 (2010), 487-502.

[64] Slonje, R.; Smith, P.K.; and Frisén, A. The nature of cyberbullying, and strategies for prevention. *Computers in Human Behavior*, 29, 1 (2013), 26-32.

[65] Smith, J.R.; Terry, D.J.; and Hogg, M.A. Social identity and the attitude–behaviour relationship: Effects of anonymity and accountability. *European Journal of Social Psychology*, 37, 2 (2007), 239-257.

[66] Spears, B.A. and Zeederberg, M. Emerging methodological strategies to address cyberbullying: Online social marketing and young people as co-researchers. In S. Bauman, D. Cross, and J. Walker (eds.), *Principles of cyberbullying research, definitions, measures, and methodology*. New York, NY: Routledge, 2013, pp. 196-209.

[67] Squicciarini, A.; Mont, M.C.; and Rajasekaran, S.D. Using modeling and simulation to evaluate enterprises' risk exposure to social networks. *Computer*, PP, 99 (2010), 1-1.

[68] Sugarman, D.B. and Willoughby, T. Technology and violence: Conceptual issues raised by the rapidly changing social environment. *Psychology of Violence*, 3, 1 (2013), 1-8.

[69] Tadmor, C. and Tetlock, P.E. Accountability. In D. Matsumoto (ed.), *The cambridge dictionary of psychology*. Cambridge, U.K.: Cambridge University Press, 2009, pp. 8.

[70] Tavani, H.T. A review of: "Cyberstalking: Harassment in the internet age and how to protect your family". *The Information Society*, 21, 5 (2005), 393-395.

[71] Tittle, C.R. *Control balance: Toward a general theory of deviance*. Boulder, CO: Westview Press, 1995.

[72] Tittle, C.R. Refining control balance theory. *Theoretical Criminology*, 8, 4 (2004), 395-428.

[73] Tittle, C.R.; Antonaccio, O.; Botchkovar, E.; and Kranidioti, M. Expected utility, self-control, morality, and criminal probability. *Social Science Research*, 39, 6 (2010), 1029-1046.

[74] Trinkle, B.S.; Crossler, R.E.; and Warkentin, M. I'm game, are you? Reducing real-world security threats by managing employee activity in online social networks. *Journal of Information Systems*, 28, 2 (2014), 307-327.

[75] Turiel, E.; Killen, M.; and Helwig, C.C. Morality: Its structure, function, and vagaries. In J. Kagan, and S. Lamb (eds.), *The emergence of morality in young children*. Chicago, IL: University of Chicago Press, 1987, pp. 155-243.

[76] Utz, S. and Beukeboom, C.J. The role of social network sites in romantic relationships: Effects on jealousy and relationship happiness. *Journal of Computer-Mediated Communication*, 16, 4 (2011), 511-527.

[77] Utz, S.; Tanis, M.; and Vermeulen, I. It is all about being popular: The effects of need for popularity on social network site use. *Cyberpsychology, Behavior, and Social Networking*, 15, 1 (2012), 37-42.

[78] Vance, A.; Lowry, P.B.; and Eggett, D. Using accountability to reduce access policy violations in information systems. *Journal of Management Information Systems*, 29, 4 (2013), 263-290.

[79] Vance, A.; Lowry, P.B.; and Eggett, D.L. A new approach to the problem of access policy violations: Increasing perceptions of accountability through the user interface. *MIS Quarterly*, 39, 2 (2015), 345–366.

[80] Walker, J.; Craven, R.G.; and Tokunaga, R.S. Introduction. In S. Bauman (ed.), *Principles of cyberbullying research: Definitions, measures, and methodology*. New York, NY: Routledge, 2013, pp. 32-34.

[81] Walther, J.B. and Bunz, U. The rules of virtual groups: Trust, liking, and performance in computer-mediated communication. *Journal of Communication*, 55, 4 (2005), 828-846.

[82] Williams, K.S. Using tittle's control balance theory to understand computer crime and deviance. *International Review of Law Computers & Technology*, 22, 1-2 (2008), 145-155.

[83] Zimbardo, P.G. The human choice: Individuation, reason and order vs. Deindividuation, impulse and chaos. In W.J. Arnold, and D. Levine (eds.), *Nebraska symposium on motivation*. Lincoln, NE: University of Nebraska Press., 1970, pp. 237-307.